Центр Непрерывного Образования и Инноваций

Основы обеспечения информационной безопасности детей

- Проблема защиты детей в Сети находит самый широкий резонанс и это не случайно. Обратимся к статистике:
- -около 50% детей выходят в Сеть без контроля взрослых.
- - 19% детей иногда посещают порносайты, еще 9% делают это регулярно.
- - 38% детей, просматривают страницы о насилии
- - 16% детей просматривают страницы с расистским содержимым
- - 25% пятилетних детей активно используют Интернет.
- -14,5% детей назначали встречи с незнакомцами через Интернет, 10% из них ходили на встречи в одиночку, а 7% никому не сообщили, что с кем–то встречаются.

- Исследователи выделяют 5 типов Интернет-зависимости у подростков:
- 1. Киберсексуальная зависимость – непреодолимое влечение к посещению порносайтов и занятия киберсексом.
- 2. Пристрастие к виртуальным знакомствам – преобладающее вирту-альное общение в чатах, форумах и т. п.
- 3. Навязчивая потребность в Сети – совершение покупок в Интернет-магазинах и участие в виртуальных аукционах, конкурсах, лотереях.
- 4. Информационная перегрузка (навязчивый web-серфинг) – бесконеч-ные путешествия по Сети, беспорядочный поиск информации.
- 5. «Гейм-зависимость» – пристрастие к компьютерным играм («стре-лялки», стратегии, квесты).

ОПАСНОСТИ ИНТЕРНЕТА

- ***Кривое зеркало» социальных сетей***

  Пользователи социальных сетей культивируют приукрашенные образы людей, и на каждом шагу видно успешных путешественников, бизнесменов, бьюти-блогеров и прочих крайне крутых персонажей. Если ребёнку не объяснить правила игры, он будет искренне верить, что так на самом деле и есть.

  А помимо успешности в соцсетях красной лентой проходит ещё одна опасная мысль: *ты ЛЕГКО тоже можешь быть таким*. Ну что сложного снять «крутой» видос?

- ***Буллинг, шантаж, доведение до суицида***

  «Травить» в школе дети могут за что угодно. Вообще никакой систематизации здесь нет. Буллинг усугубляется соцсетями и мессенджерами, когда ребёнок после школы не получает паузу для психики, потому что травля из мира реального перетекает в Интернет. Попробуйте сами быть под жёстким прессингом почти всё время, что не спите. Долго ли выдержите? А теперь представьте, каково может быть ребёнку, который по какой-то причине стесняется или не хочет спросить совета родителей.

  Любопытство. На каком-то этапе взросления всё, что опасно автоматически может причисляться к крутому. Когда-то круто было иметь «Поваренную книгу Анархиста» или «Лики смерти». А вот не так давно «модно» было проверить свои нервы в игре «Синий кит». «Разбуди меня в 4:20» и вот это вот всё. Помните? Дети из любопытства сами могут вляпаться во что-то, а потом из-за впечатлительности и страха не рассказать о наступивших проблемах.

1. Спросите ребенка, какие приложения и веб-сайты он использует

Попросите ребенка научить вас использовать и показать свои любимые приложения, игры или веб-сайты. Это поможет вам понять, как они работают, и выявить потенциальные риски с худшими приложениями для детей.

2. Обсудите с вашим ребенком все возможные проблемы

Если вы опасаетесь, что ребенок использует неподходящее для детей и подростков приложение или сайт, поделитесь с ним своим беспокойством. По возможности принимайте совместное с ребенком решение, чтобы он понимал причины, по которым не следует использовать то или иное приложение.

3. Будьте честны и откровенны с ребенком

Поговорите с ним о последствиях ненадлежащего использования технологий. Расскажите ему о кибербуллинге, взломе, социальной инженерии и онлайн-ухаживаниях.

4. Убедите ребенка, что с вами всегда можно поделиться

Скажите ребенку, что вы не будете остро реагировать, если он сообщит вам о том, что видел в Интернете: например, неприятные комментарии, материалы сексуального характера или изображения насилия. Скажите также, что вы бы предпочли, чтобы он сообщил об этом вам, а не держал в себе. Покажите, как можно блокировать нежелательный контент или сообщать о нем.

5. Установите границы, но будьте реалистом

Устанавливаемые границы использования интернета должны зависеть от возраста ребенка и того, что приемлемо в вашей семье. Границы могут включать согласование следующих правил: сколько времени ребенок может проводить в сети и когда, не писать текстом вещи, которые он не сказал бы в лицо, не отправлять личные изображения, не сообщать вам пароль, чтобы вы могли проверить телефон ребенка.

6. Настройте родительский контроль

Настройте или пересмотрите параметры родительского контроля и интернет-фильтры. Родительский контроль предназначен для защиты детей от неприемлемого контента в интернете. Его можно использовать по-разному, например, чтобы обеспечить детям доступ только к соответствующему возрасту контенту, установить время использования устройства, отслеживать активность и не допустить передачу личной информации посторонним.

7. Убедитесь, что на устройстве ребенка установлены последние версии антивирусных программ

Антивирусные программы защищают устройства от внешних атак, находят и уничтожают потенциальные угрозы для системы и предупреждают о них. Новые вирусы появляются постоянно, и разработчики регулярно улучшают антивирусы, чтобы они оставались эффективными.

8. Убедитесь, что для ребенка установлены настройки максимальной конфиденциальности

Почти все приложения для социальных сетей имеют настраиваемые параметры конфиденциальности. Изучите их и вместе с ребенком настройте профили.

9. Используйте надежное решение кибербезопасности на устройствах детей