**«Информационная безопасность дошкольников»**

Данная тема актуальна для всей России, поскольку в России 85% российских детей в возрасте от 10 до 17 лет активно пользуются Интернетом. По статистическим данным в Сети они проводят до 25 часов в неделю и, как правило, пользуются Интернетом бесконтрольно. В современных условиях развития общества компьютер стал для ребенка и «другом», и «помощником», и даже «воспитателем», «учителем».

Существует ряд аспектов при работе с компьютером, а в частности, с сетью Интернет, негативно влияющих на физическое, моральное, духовное здоровье подрастающего поколения, порождающих проблемы в поведении у психически неустойчивых школьников, представляющих для детей угрозу.

**Мощное воздействие на детей, их нравственные установки оказывает широко распространяемая кино- и видеопродукция, напичканная сценами убийств, грабежей, разбоев, хулиганства, изнасилований, самоубийств и других преступных и антиобщественных проявлений.**

**В связи с этим необходимо направить все усилия на защиту детей от информации, причиняющей вред их здоровью и развитию. Просвещение подрастающего поколения, знание ребенком элементарных правил отбора информации, а также умение ею пользоваться способствует развитию системы защиты прав детей.**

Зачастую дети принимают всё, что видят по телевизору и в Интернете, за чистую монету. **В силу возраста, отсутствия жизненного опыта и знаний в области медиаграмотности они не всегда умеют распознать манипулятивные техники, используемые при подаче рекламной и иной информации, не анализируют степень достоверности информации и подлинность ее источников. Поэтому проблема защиты физического и духовно-нравственного здоровья детей в современной медиа-среде становится все более актуальной в связи с тем, что возраст, в котором человек начинает работать с Интернет, становится все моложе, а численность несовершеннолетних пользователей увеличивается.**

***Угрозами информационно-психологической безопасности детей является:***

1. Получение детьми непристойных (то есть не соответствующих принятым стандартам нравственности) материалов различного характера (например, порнографии, материалов, содержащих жестокость и ненормативную лексику, вульгарные или шокирующие выражения);

2. Получение детьми материалов, в содержании которых отражается национальная или другая (например, религиозная, социальная) нетерпимость и пропаганда расового, национального и религиозного неравенства или антиобщественного поведения;

3. Получение детьми материалов, содержащих рекламу и пропаганду опасной и вредной для здоровья человека продукции (например, алкоголя, табачных изделий, наркотических веществ).

Современные дети и подростки, которых называют «цифровыми гражданами» легко осваивают компьютер, мобильные устройства и умело пользуются ими. При этом навыки детей в области безопасности в Интернете отстают от их способности осваивать новые приложения и устройства.

**Основные опасности в Интернете для детей и подростков следующие:**

1. Кибербуллинг (интернет-травля).

2. Использование Интернета для манипуляции сознанием детей и подростков (пропаганда экстремистского, антисоциального поведения, суицидов, вовлечение в опасные игры).

3. "Незнакомый друг" в социальных сетях.

4. Кибермошенничество.

5. Безопасность доступа в Сеть и кража личных данных техническими средствами.

6. Незаконный сбор персональных данных несовершеннолетних и (или) распространение их в открытом доступе.

7. Просмотр сайтов для взрослых +18

**1. Кибербуллинг (интернет-травля).Кибербуллинг: как обезопасить ребенка в cети**

Большинство соцсетей не разрешает создавать собственные аккаунты детям до 13 лет. Младшие школьники, как правило, присутствуют в соцсетях под присмотром взрослых и реже сталкиваются с кибербуллингом и киберагрессией. В этом случае полезно заранее рассказать детям о том, как общаться в сети безопасно и что делать, если они столкнулись с киберагрессией.

Что такое кибербуллинг и его разновидности. Кибербуллинг-это травля человека по интернету.В переводе с анг.яз кибер это означает все ,что связано с интернетом,а слово буллинг от анг.«bull»-быкпереводится как травля,приставание,или более достоверно «быкование». кибербуллинг совершается группой пользователей;агрессивные действия продолжаются и повторяются в течение определенного времени;

Травля в детских коллективах — это нередкое явление. Кибербуллинг часто становится продолжением травли в реальной жизни. Жертвой при этом может стать любой человек вне зависимости от пола и возраста. В этом нет его вины. Это травля пользователя через все каналы сетевого общения: социальные сети, форумы, чаты, мессенджеры. Проводить кибербуллинг (другое название - троллинг) могут как одноклассники, интернет-друзья и т.д., так и совершенно посторонние люди.

«Троллинг» может принимать разные формы: оскорбления через личные сообщения, публикация и распространение конфиденциальной, провокационной информации о жертве. В интернете, как правило, ребенок находится один на один с потенциальным обидчиком, который к тому же уверен в своей анонимности и может действовать более нагло.Травля может происходить где угодно и принимать различные формы — от распространения слухов и размещения нежелательных фото до угроз в чей-то адрес. Под травлей понимается умышленное оскорбление, запугивание и угнетение состояния других людей."

**Поэтому самую важную роль в защите ребенка от кибер-террора играют отношения с родителями**

**троллинг** (оскорбления, обидные сообщения и фото в публичном пространстве: в социальных сетях, группах, на сайтах);

**хейтинг** (негативные комментарии и сообщения, в которых агрессор демонстрирует ненависть, критикует и ругает без объяснений);

**флейминг** (скандал на публике, когда большое количество людей присоединяется к одной обвинительной стороне и накидывается на другую, участники стараются друг друга унизить);

**киберсталкинг** (преследование в социальных сетях через повторяющиеся угрожающие, вызывающие тревогу и раздражение сообщения, при этом цель агрессора — напугать получателя, начать его контролировать);

**грифинг** (целенаправленное преследование одних игроков другими в онлайн-играх, чтобы лишить жертву удовольствия от игры);

**секстинг** (рассылка и публикация фото- и видеоматериалов интимного содержания);

**создание фейковых аккаунтов** (под вымышленными именами агрессоры выведывают у пострадавшего конфиденциальную информацию и распространяют ее);

**взлом и подделка аккаунтов жертвы** (цель таких действий — опорочить репутацию, выведать секреты и создать неверное впечатление о человеке);

**Что делать, если ребенка травят**

* отправлять жалобу на оскорбительные или неуважительные комментарии, сообщения, фото, аккаунты и группы;
* блокировать обидчиков, не боясь обидеть или выглядеть неудобным;

Очень важно, чтобы дети не оставались молчаливыми свидетелями кибербуллинга, знали, у кого они могут попросить помощи и сообщали об агрессивном поведении в соответствующие службы поддержки социальных сетей. Чем активнее свидетели поддерживают пострадавшую сторону, тем выше вероятность того, что агрессор остановит травлю. Поддержка также помогает избежать тяжелых психологических последствий кибербуллинга — дает ощущение, что пострадавший не один на один с этой ситуацией.

**Если ребенок столкнулся с кибербуллингом, используйте следующие рекомендации:**

Если аккаунт ребенка кто-то пытался взломать, закройте его профиль от посторонних лиц в настройках конфиденциальности; изучите подписчиков и удалите людей, которых ребенок не знает лично, с которыми он в конфликте или кого подозревает в травле.

В настройках безопасности добавьте двухфакторную аутентификацию; смените пароли после попытки взлома; отмените возможность сохранять входы; добавьте резервную почту для восстановления пароля.

Убедитесь, что пароли в социальных сетях и электронной почте достаточно сложные и отличаются.

Если вы или ребенок увидели чужой профиль, в котором используются данные ребенка (имя, фото, видео), пожалуйтесь на страницу-клона и попросите сделать это друзей; чаще всего агрессоры берут информацию о пострадавшей стороне с ее же страницы — лучше закрыть профиль от посторонних глаз.

Расскажите ребенку, что не стоит отправлять кому-либо в интернете свои фото, видео и другую личную информацию; научите обозначать свои границы словами «Я такое не отправляю, мне это не интересно, я не хочу об этом говорить»; дети часто боятся обидеть новых друзей — объясните, что не стоит приносить в жертву собственную безопасность ради спокойствия другого человека.

Исчезающие сообщения и быстрое удаление отправленного не обеспечивает безопасность — агрессор может сделать снимок экрана, медиафайлы могут сохраняться автоматически даже после того, как ребенок их удалил у всех участников беседы.

Если ребенок столкнулся с преследователем, помогите ему немедленно блокировать все аккаунты, связанные с агрессором; удалите из открытого доступа геометки и любые указания на то, где ребенок живет, учится, бывает; предупредите друзей и знакомых о существовании преследователя.

При наличии угроз и киберпреследования обратитесь в полицию.

В случае интенсивной вербальной агрессии в мессенджерах или соцсетях поддержите ребенка; нет смысла вступать с хейтером или троллем в диалог; заблокируйте агрессорам доступ к профилю ребенка в соцсети, удаляйте сообщения от агрессоров, отправьте их в черный список.

Если агрессивных сообщений много и удалить их возможности нет, помогите ребенку игнорировать автора — скажите, что не стоит верить каждому написанному сообщению и искать в нем правду; ребенку очень нужна ваша поддержка.

Если ребенок уже отправил личную информацию кому-то, помогите ему удалить то, что возможно удалить; все, что попадает в интернет, остается там навсегда; это не катастрофа — ребенку понадобится поддержка близких и друзей, чтобы справиться с ситуацией, если чувствительная информация будет обнародована; в некоторых случаях стоит удалить аккаунты ребенка в социальных сетях, чтобы оградить его от негативной информации, а также чтобы агрессор не имел возможности отмечать ребенка на фото и видео.

**Общие правила безопасности в интернете**

Общение в интернете можно сравнить с прогулкой на улице: лучше сначала выходить в виртуальный мир вместе с ребенком. Объясните ребенку, как устроено виртуальное общение, и научите его обозначать личные границы в сети. Общие правила безопасности хорошо работают в виртуальной реальности. Везде, где есть возможность общения (в мессенджерах, социальных сетях, сетевых играх), ребенок может встретиться с киберагрессией. Покажите ему, как вы сами обеспечиваете свою безопасность в интернете, и научите его следовать общим советам:

* сохраняйте приватность и избегайте распространения персональных данных, особенно тех данных, по которым вас легко найти;
* не отправляйте свои фото даже в ответ на подобную просьбу;
* контролируйте общение в сети, для блога заведите публичный профиль, а общение с друзьями и знакомыми ведите из личного аккаунта, который будет скрыт от посторонних глаз, в котором информация о вас будет недоступна незнакомым людям;
* контролируйте тех, кого добавляете в друзья и подписчики;
* не ведитесь на хейт и троллинг, блокируйте обидчиков, жалуйтесь на негативные комментарии в соцсетях;
* общайтесь уважительно и в удовольствие, а также не забывайте про бдительность.
* Кибербуллинг, как и травля в реальной жизни, может иметь психологические последствия для ребенка. Дети часто не склонны делиться со взрослыми своими проблемами в сетевом общении, так как не могут оценить серьезность ситуации, хотят справиться самостоятельно или боятся ограничений со стороны родителей. Расскажите ребенку о базовых правилах безопасности в сети, обсуждайте с ним его опыт общения с сетевыми знакомыми. Если ребенок оказался в ситуации кибербуллинга, напомните ему, что он ни в чем не виноват, поддержите и помогите справиться с последствиями. Видов кибербуллинга много, невозможно быть готовым ко всему.

**2. Использование Интернета для манипуляции сознанием детей и подростков (пропаганда экстремистского, антисоциального поведения, суицидов, вовлечение в опасные игры).**

Руководитель Центра защиты детей от интернет-угроз Владимир Рогов, сказал следующее, что в настоящее время особо актуальной становится проблема защиты детей от информации, распространяемой в так называемых закрытых группах, провоцирующих детей на суицид. Председатель Следственного комитета РФ Александр Бастрыкин сообщил, что сегодня всё большую опасность стали представлять собой "игры на выживание" или "игры на вымирание", организованные в интернете создателями так называемых "групп смерти". "Каждый день сотрудниками Главного управления криминалистики Следственного комитета Российской Федерации выявляются все новые и новые сообщества, которые ставят своей целью уничтожение молодежи. Смысл групп тот же — оторвать ребёнка от своего окружения (родители, друзья), приманить к себе, переделать в новый формат

**3. "Незнакомый друг" в социальных сетях**

Исследования показывают, что среди людей, которые заходят на страничку ребенка в соцсетях, каждый второй — это человек, которого он никогда в своей жизни не видел

Важно, чтобы дети ценили приватность своего пространства в интернете точно так же, как ценят приватность своего личного пространства дома...

Ребенок может передать незнакомцам свои персональные данные, поделиться номером кредитки мамы, может сфотографировать квартиру, сообщить адрес, показать интерьер и ценные вещи, рассказать, что семья уезжает в отпуск, и т. д. Нужна очень серьезная кооперация всей семьи, чтобы уяснить: все, что мы выкладываем в интернет, становится достоянием огромного круга людей, которые далеко не всегда дружелюбно настроены.

**4. Просмотр сайтов для взрослых**

По результатам исследования «Лаборатории Касперского», из всех сайтов с маркировкой 18+ наибольший интерес для российских детей представляют эротические и порнографические сайты ,на втором месте оружейная тематика ,на третьем - нецензурная лексика .

Чего хочется большинству детей? Поскорее стать взрослыми. И любая маркировка "только для взрослых" еще больше разжигает интерес, считают психологи

Вывод исследования очевиден - Безопасность ребенка в Сети = Контроль со стороны родителей + «Родительский контроль»

**Итог**

 Создайте «детский» профиль пользователя на вашем ПК или ноутбуке, где будут лишь предназначенные для детей материалы (например, мультфильмы).

 Научите ребенка пользоваться социальными сетями и поисковыми сервисами. Заведите ему страничку в соцсетях и адрес электронной почты. Используйте разные пароли!

 Используйте настройки безопасности/приватности выбранных сайтов для ограничения доступа к личным данным вашего ребенка.

 Проверяйте возрастные ограничения сайтов и видеоигр. Многие из них не предназначены для несовершеннолетних.

 Объясните, что в интернете, как и в реальной жизни, не стоит общаться с незнакомыми людьми и тем более раскрывать информацию о себе или семье.

 Даже друзьям и знакомым не следует доверять на 100% – профиль одноклассника вашего ребенка может быть взломан злоумышленниками.

 Приглядывайте за тем, кого ваш ребенок добавляет в друзья в соцсетях и что публикует в открытом доступе.

 Если вашего ребенка в интернете кто-то напугал или расстроил – он должен знать, что в любой момент может прийти к вам и рассказать об этом.

 Убедитесь, что в вашей семье компьютеры, ноутбуки и мобильные устройства защищены антивирусным ПО.  Активируйте в вашем антивирусном продукте функцию «Родительский контроль» и определите категории сайтов, которые необходимо блокировать (онлайн-магазины, казино, XXX-сайты и др).

**ПАМЯТКА по безопасности детей в сети Интернет**

Классификация интернет-угроз Во Всемирной паутине существует следующие виды опасности юных пользователей:

• суицид-сайты;

• сайты-форумы потенцинальных самоубийц;

• наркосайты (интернет пестрит новостями о «пользе» употребления марихуаны, рецептами и советами изготовления «зелья»);

• сайты, разжигающие национальную рознь и расовое неприятие (экстремизм, национализм, фашизм);

• сайты порнографической направленности;

• сайты знакомств (виртуальное общение разрушает способность к реальному общению, у подростков теряются коммуникативные навыки);

• сайты, пропагандирующих экстремизм, насилие и девиантные формы поведения, прямые угрозы жизни и здоровью школьников от незнакомцев, предлагающих личные встречи, а также различные виды мошенничества;

• секты (виртуальный собеседник может повлиять на мировоззрение подростка).

**Правила работы в сети Интернет**

1. Не входите на незнакомые сайты.

2. Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на вирусы

. 3. Если пришло незнакомое вложение, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину.

4. Никогда не посылайте никому свой пароль.

5. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв.

6. При общении в Интернет не указывайте свои личные данные, а используйте псевдоним (ник)

7. Без контроля взрослых ни в коем случае не встречайтесь с людьми, с которыми познакомились в сети Интернет.

8. Если в сети необходимо пройти регистрацию, то должны сделать ее так, чтобы в ней

не было указано никакой личной информации.

9. Не всей информации, которая размещена в Интернете, можно верить.

10. Не оставляйте без присмотра компьютер с важными сведениям на экране

11. Не сохраняйте важные сведения на общедоступном компьютере.

**Вывод.**

Действительно, информационные и коммуникационные технологии открывают уникальные возможности для системы образования, вместе с тем все большую актуальность приобретает проблема безопасности ребенка в информационном обществе отличающегося информационной насыщенностью и интенсивностью, многоканальностью влияний, многообразием транслируемых ценностей. Вы, уважаемые родители должны помнить о чрезвычайной опасности, которая кроется не столько в самом компьютере, сколько в доступной для всех желающих информации, размещенной в сетях.