МВД России

УПРАВЛЕНИЕ МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ЯМАЛО-НЕНЕЦКОМУ АВТОНОМНОМУ ОКРУГУ
(УМВД России по Ямало-Ненецкому автономному округу)

ул. А.Матросова, 7, Салехард, 629008
тел. (349-22) 4-45-90, факс 4-13-60

29.08.2019 № 74/22-6712

На № _____ от _____

Директору департамента по взаимодействию с федеральными органами государственной власти и мировой юстиции Ямало-Ненецкого автономного округа

А.В. Копырину

Матросова ул., д. 7, корп. 1, г. Салехард

О направлении информации

Уважаемый Андрей Вячеславович!

Во исполнение п. 2.2. Протокола совместного заседания экспертного совета по противодействию идеологии терроризма при антитеррористической комиссии в Ямало-Ненецком автономном округе и рабочей группы по вопросам профилактики экстремизма от 20 декабря 2018 года № 2, направляю в Ваш адрес рекомендации для школьников и их родителей, посвященные безопасному поведению в сети Интернет в целях их возможного направления в органы местного самоуправления.

Рекомендации подготовлены ЦПЭ УМВД России по Ямало-Ненецкому автономному округу с использованием сведений, предоставленных Департаментом образования округа (исх. рег. № 801-12-05/427 от 22.08.2019) и информационных материалов, подготовленных ГУ МВД России по Красноярскому краю

Приложение: 1. Лекция для родителей, на 13 листах.
2. Лекция для учащихся, на 5 листах.
3. Памятка для родителей, на 5 листах.
4. Памятка для учащихся, на 5 листах.

Врио заместителя начальника Управления - начальника полиции Д.А. Лебедев

ПЛАН-КОНСПЕКТ

Тема: «Безопасность детей в Интернете».
Лекция для родителей.

Интернет постепенно проникает в каждую организацию, общественное учреждение, учебное заведение, в наши дома. Число пользователей Интернета в России стремительно растет, причем доля молодежи и совсем юной аудитории среди пользователей. Всемирной паутины очень велика. Для многих, особенно молодых людей, он становится информационной средой, без которой они не представляют себе жизнь. И это неудивительно: ведь в Интернете можно найти информацию для реферата или курсовой, послушать любимую мелодию, купить понравившуюся книгу или обсудить горячую тему на многочисленных форумах. Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но - как и реальный мир - Сеть тоже может быть опасна: в ней появились своя преступность, хулиганство, вредительство и прочие малоприятные явления. Виртуальность общения предоставляет людям с недобрыми намерениями дополнительные возможности причинить вред детям. В последнее время в Интернете появляется много материалов агрессивного и социально опасного содержания. Взрослым нужно помнить о существовании подобных угроз и уделять повышенное внимание вопросу обеспечения безопасности детей в Интернете.

К настоящему времени проблема безопасности детей в Интернете, без преувеличения, стала глобально значимой проблемой. Лидеры по внедрению информационных технологий в повседневную жизнь и нормативному регулированию информационных отношений уже вплотную столкнулись с необходимостью решения всего спектра проблем: как регулировать доступ детей в Интернет и контролировать их пребывание в Интернете? Как защищать детей от преступных действий со стороны злоумышленников, которые очень активно используют Интернет для своих вредных, незаконных и аморальных целей?

Сегодня в мире уже возникло устойчивое понимание того, что проблема детской безопасности в Интернете - это предмет, требующий скоординированного решения на всех уровнях: от семейного и муниципального до регионального и международного. В решении этой проблемы необходимо действовать системно и использовать не только правовые регуляторы, но и нормы обычаев и морали, а также технические и технологические возможности. Новым и самым эффективным механизмом решения этой проблемы может и должно стать формирование информационной культуры личности - родителей и детей, а также профессиональной информационной культуры журналистов и учителей.

Родители должны понимать, какая информация нужна ребенку для развития. Одно дело - найти хорошую книгу и подтолкнуть ребенка к диалогу с ней, но что, если искомая информация находится в Интернете? Тогда нужно сесть вместе с ребенком к компьютеру и попытаться найти ее вместе.

В этом случае ребенок будет позитивно учиться искать, находить и использовать информационные ресурсы и технологии. Надо с первого знакомства с информационными технологиями разъяснять ребенку, как ему жить в информационном пространстве, как избирательно подходить к информации в открытой информационной среде. Важно, чтобы и сами родители, и дети понимали, что в информационном пространстве есть свои плюсы и минусы, плохое и хорошее.

Пользуясь возможностями Интернета, дети подвергаются опасности вступить в контакт со злоумышленниками. Анонимность общения в Интернете способствует быстрому возникновению доверительных и дружеских отношений. Преступники используют преимущества этой анонимности для завязывания отношений с неопытными молодыми людьми.

Вы сможете защитить своих детей, если поймете возможную опасность общения через Интернет и будете в курсе того, чем они занимаются в Сети.

Преступники преимущественно устанавливают контакты с детьми в чатах, при обмене мгновенными сообщениями, по электронной почте или на форумах. Для решения своих проблем многие подростки обращаются за поддержкой на конференции. Злоумышленники часто сами там обитают; они стараются привлечь подростка своим вниманием, заботливостью, добротой и даже подарками, нередко затрачивая на эти усилия значительное время, деньги и энергию. Обычно они хорошо осведомлены о музыкальных новинках и современных увлечениях детей. Они выслушивают проблемы подростков и сочувствуют им. Но постепенно злоумышленники вносят в свои беседы оттенок сексуальности или демонстрируют материалы откровенно эротического содержания, пытаясь ослабить моральные запреты, сдерживающие молодых людей. Некоторые преступники могут действовать быстрее других и сразу же заводить сексуальные беседы. Преступники могут также оценивать возможность встречи с детьми в реальной жизни.

КАК УЗНАТЬ, НЕ СТАЛ ЛИ ВАШ РЕБЕНОК ПОТЕНЦИАЛЬНОЙ ЦЕЛЬЮ ПРЕСТУПНИКА?

Приведенные ниже признаки могут означать, что на вашего ребенка обратил внимание злоумышленник.

Ваш ребенок проводит много времени в Интернете.

Дети, преследуемые Интернет - преступниками, проводят большое количество времени в Сети, особенно в чатах; подчас закрывают дверь в свою комнату и скрывают, чем они занимаются, сидя за компьютером. В семейном компьютере появились материалы откровенного содержания. В качестве предлога для начала сексуальных обсуждений злоумышленники могут снабжать детей фотографиями, ссылками на соответствующие сайты и присылать сообщения эротической окраски.

Вашему ребенку звонят люди, которых вы не знаете, или он сам звонит по номерам, которые вам не знакомы. Установив в Интернете контакт с вашим ребенком, некоторые злоумышленники могут попытаться вовлечь детей в секс по телефону или попытаться встретиться в реальной жизни. Если дети не решаются дать номер телефона, злоумышленник может сообщить им свой. Не разрешайте своему ребенку лично встречаться с незнакомцем без контроля с вашей стороны.

Ваш ребенок получает письма, подарки или посылки от неизвестного вам лица. Обычно преследователи посылают своим потенциальным жертвам письма, фотографии и подарки. В других странах они порой даже отправляют билеты на самолет, чтобы соблазнить ребенка личной встречей.

Ваш ребенок сторонится семьи и друзей и быстро выключает монитор компьютера или переключается на другое окно, если в комнату входит взрослый. Интернет-преступники усердно вбивают клин между детьми и их семьями и часто преувеличивают небольшие неприятности в отношениях ребенка с близкими. Кроме того, дети, подвергающиеся сексуальному преследованию, становятся замкнутыми и подавленными.

Ваш ребенок использует чью-то чужую учетную запись для выхода в Интернет. Даже дети, не имеющие доступа в Сеть дома, могут встретить преследователя, выйдя в Интернет у друзей или в каком-нибудь общественном месте, например библиотеке. Иногда преступники предоставляют своим жертвам учетную запись, чтобы иметь возможность с ними общаться.

ЧТО ДЕЛАТЬ, ЕСЛИ ВАШ РЕБЕНОК СТАЛ ПОТЕНЦИАЛЬНОЙ ЦЕЛЬЮ ПРЕСТУПНИКА?

Регулярно проверяйте компьютер на наличие материалов откровенного характера или каких-либо свидетельств об общении с сексуальной окраской - это настораживающие признаки.

Контролируйте доступ вашего ребенка ко всем средствам общения, работающим в режиме реального времени, таким, как чаты, мгновенные сообщения и электронная почта. Обычно Интернет-преступники впервые встречают своих потенциальных жертв в чатах, а затем продолжают общаться с ними посредством электронной почты или мгновенных сообщений. Не вините детей. Если, несмотря на все меры предосторожности, ваши дети познакомились в Интернете со злоумышленником, вся полнота ответственности всегда лежит на правонарушителе. Предпримите решительные действия для прекращения дальнейших контактов ребенка с этим лицом.

Если ваш ребенок получает фотографии откровенного характера или подвергается сексуальным домогательствам, сохраните всю имеющуюся информацию, включая адреса электронной почты, адреса сайтов и чатов, чтобы иметь возможность ознакомить с ней представителей правоохранительных органов.

ЧТО ТАКОЕ НЕЖЕЛАТЕЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ?

Объясните детям, что под выражением «нежелательное программное обеспечение» понимаются программы, которые выполняют на компьютере некие задачи без вашего согласия. Они могут показывать рекламные сообщения, объявления или собирать личные данные о вас и вашей семье.

Нужно помнить, что ничто не может дать стопроцентной гарантии защиты вашего компьютера. Поэтому в любом случае вы и ваши дети должны быть крайне внимательны к получению сообщений от неизвестного адресата с вложением. Практически все вирусы не могут распространяться, пока вы не откроете или не запустите инфицированную программу.

Если дети регулярно пользуются компьютером, они могут забрести на сайты или скачать файлы, которые могут заразить компьютер. Иногда ваши дети могут случайно заразить компьютер программой-шпионом, даже не осознавая этого.

АЗАРТНЫЕ ИГРЫ В ИНТЕРНЕТЕ: КАК ПРЕДОСТЕРЕЧЬ ДЕТЕЙ? В ЧЕМ СОСТОИТ ОТЛИЧИЕ МЕЖДУ ИГРОВЫМИ И САЙТАМИ С АЗАРТНЫМИ ИГРАМИ. Множество детей обожают искать развлечения (например, игры) в Интернете. Иногда при поиске нового игрового сайта они могут попасть на карточный сервер. Большинство игр и развлечений для несовершеннолетних вполне законны, однако им нельзя играть в азартные игры на деньги. Разница между игровыми сайтами и сайтами с азартными играми состоит в том, что на игровых сайтах обычно содержатся настольные и словесные игры, аркады и головоломки с системой начисления очков. Здесь не тратятся деньги: ни настоящие, ни игровые. Сайты с азартными играми могут допускать, что люди выигрывают или проигрывают игровые деньги.

ПРЕДОСТЕРЕЧЬ ДЕТЕЙ ОТ ИГР НА ДЕНЬГИ?

Родители должны решить, во что можно играть их детям. Обсудите жанр игр (скажем, только бильярд, стратегии и шахматы) и количество участников (можно ведь играть и одному). Напоминайте детям, что им нельзя играть на деньги. Предложите им играть в не менее увлекательные игры, но которые не предполагают использование наличных или безналичных проигрышей/выигрышей. Помогите детям понять механизм таких игр. Ведь в основном подобные развлечения используются создателями для получения прибыли. Игроки больше теряют деньги, нежели выигрывают.

Не позволяйте детям использовать номера ваших кредитных карт в Интернете. Держите их в недоступном для детей месте. В сетевых играх на деньги они обычно требуются. Дети могут ненароком влезть в долги. Объясните, что к играм на деньги можно пристраститься. Всегда есть опасность приобретения зависимости. Это как болезнь. Особенно если есть кредитная карта и положительный баланс на ней; человек может играть, пока не истратит все до конца. Контролируйте поведение своих детей в Интернете. Следите за тем, какие сайты посещают ваши дети и что они делают в Интернете.

В ЧЕМ СОСТОИТ ОБЩЕНИЕ ДЕТЕЙ В ЧАТАХ И СИСТЕМАХ ОБМЕНА МГНОВЕННЫМИ СООБЩЕНИЯМ?

Возможно, вы слышали о чатах, в которых люди встречаются для обмена сообщениями на определенную тему. Может быть, вы даже сами там общались. Комнаты чата, в которых происходит общение, представляют собой виртуальные помещения в Сети, в которых люди могут набирать сообщения, почти мгновенно появляющиеся на экранах компьютеров других участников. Чаты обычно являются анонимными, поскольку участники пользуются псевдонимами.

В Интернете существует множество чатов различной направленности. В них предоставляется потрясающая возможность обсуждать разные темы с людьми со всего мира. Чаты очень популярны среди детей, и, к сожалению, преступникам это известно. Поэтому эта форма общения представляет особенную опасность для детей и подростков.

Многие люди, говоря об общении в системе обмена мгновенными сообщениями, называют это общением в чате, однако все же существует небольшая разница. Первая обычно используется для беседы между двумя собеседниками, в то время как в чате идет разговор с группой людей, но основные правила безопасности остаются одними и теми же.

КАК СДЕЛАТЬ ОБЩЕНИЕ В ИНТЕРНЕТЕ КОМФОРТНЫМ?

Контролируйте использование чата вашим ребенком. Помните о том, что дети могут участвовать в чатах, расположенных на сайтах, при помощи программ поддержки чатов, сотовых телефонов и даже некоторых онлайновых игр.

Добейтесь того, чтобы дети никогда не сообщали в чатах свои личные данные. Так, при выборе псевдонима необходимо выбирать имя, не выдающее личные данные детей. Следует настоять на том, чтобы дети не посылали своих фотографий тем, с кем они познакомились в чате.

Предупредите ребенка о том, что, если что-либо в чате вызовет у него чувство дискомфорта, необходимо немедленно его покинуть и сообщить о происшедшем кому-нибудь из взрослых. Пусть дети всегда сообщают вам об участниках чата, которые предлагают им встретиться в приватных комнатах чата. У детей должно быть настороженное отношение к попыткам собеседников перевести общение из виртуальной плоскости в реальную. Им никогда нельзя соглашаться на личную встречу с незнакомыми людьми, с которыми они познакомились в Интернете.

ИНТЕРНЕТ-ДНЕВНИКИ: ОСНОВЫ БЕЗОПАСНОГО ВЕДЕНИЯ

Последние исследования показывают, что сегодня примерно половина всех веб-журналов принадлежат подросткам. При этом двое из трех раскрывают свой возраст; трое из пяти публикуют сведения о месте проживания и контактную информацию, а каждый пятый сообщает свое полное имя. Не секрет, что подробное раскрытие личных данных потенциально опасно.

При этом все больше молодых пользователей создают собственные дневники, и каждый стремится привлечь как можно больше внимания аудитории. Иногда это приводит к тому, что дети размещают в блогах такой неуместный материал, как провокационные фотографии - свои или друзей.

Требуйте от ваших детей никогда не публиковать в них какую-либо личную информацию, в том числе фамилию, контактную информацию, домашний адрес, номера телефонов, название школы, адрес электронной почты, фамилии друзей или родственников, свои имена в программах мгновенного обмена сообщениями, возраст или дату рождения.

Требуйте от ваших детей никогда не помещать в журнале провокационные фотографии, свои или чьи-либо еще, и всегда проверять, не раскрывают ли изображения или даже задний план фотографий какую-либо личную информацию. Пусть ваши дети знают, что публикуемая в Интернете информация остается там надолго и кто угодно может легко распечатать веб-журнал или сохранить его на своем компьютере.

Рекомендуйте детям пользоваться веб-журналами только с ясно сформулированными условиями использования и проверять, можно ли защитить с помощью пароля сами веб-журналы, а не только учетные записи пользовател.

Рекомендуйте вашим детям не стремиться соревноваться с другими детьми, ведущими веб-журналы.

Пусть дети стараются вести свой блог в положительном ключе и не использовать его для злословия или нападок в адрес других.

КТО ТАКИЕ ИНТЕРНЕТ-ХУЛИГАНЫ И ЧТО ОНИ ДЕЛАЮТ?

Их называют гриферами, задирами, дурными игроками, повернутыми и т.д. Есть вероятность, что один из таких злодеев по крайней мере единожды побеспокоит вашего ребенка в играх. Обидчики (гриферы), по сути, те же дворовые хулиганы; они получают удовольствие, хамя и грубя окружающим. Обычно хулиганы издеваются над другими, особенно над начинающими (чайниками); мешают играть товарищам по команде; используют нецензурную лексику; жульничают; создают вместе с другими гриферами бродячие банды; блокируют выходы из комнат; выманивают монстров на неосторожных игроков или используют игру, чтобы досаждать, кому только можно, или изводить конкретного человека. Хотя они составляют лишь малую часть от общего числа пользователей, из-за гриферов некоторые компании потеряли клиентов. В итоге многие разработчики игр не жалеют этих хулиганов и используют любые методы для их вычисления.

Пусть ваши дети их игнорируют. Если ребенок не будет реагировать на их воздействия, большинству гриферов это, в конце концов, надоест и они уйдут. Посоветуйте детям изменить параметры игры. Добейтесь, чтобы ребенок играл в игры, правила или режимы которых можно изменить.

Таким образом, тактика гриферов становится бессмысленной.

Пусть дети играют на сайтах со строгими правилами. Там, где установлены строгие правила, администратор сможет немедленно заблокировать хулиганов.

Пусть играют в игры, где от гриферов можно легко избавиться. Предложите ребенку играть в те игры, где сообщения хулиганов можно отключить или проголосовать за их исключение из игры. Придумайте еще что-нибудь. Если обидчик продолжает беспокоить вашего ребенка, добейтесь, чтобы он сменил игру или сделал перерыв и вернулся позже. Сообщайте о «дырах» в игре. Поищите вместе с ребенком уязвимости в игре или новые способы жульничества. Сообщайте о своих находках администратору.

Пусть ваши дети воздерживаются отвечать огнем на огонь. Убедитесь, что ребенок не использует против обидчиков их же тактику; скорее всего, это спровоцирует гриферов на еще более озлобленное поведение. Или, что еще хуже, создаст о ребенке впечатление как об обидчике.

Рекомендуйте детям избегать провокаций с именами. Ребенок избежит многих проблем, если не станет использовать псевдоним, который может спровоцировать обидчика. Пусть дети не выдают личную информацию. Хулиганы (да и вообще кто угодно) могут использовать настоящие имена, номера телефонов, а также домашние или электронные адреса, чтобы причинить ребенку неприятности.

МАТЕРИАЛЫ НЕЖЕЛАТЕЛЬНОГО СОДЕРЖАНИЯ: КАК ИЗБЕЖАТЬ? ЧТО ЗНАЧИТ НЕЖЕЛАТЕЛЬНОЕ СОДЕРЖАНИЕ.

Как правило, большинство родителей не склонны поощрять знакомство своих детей с материалами порнографического, ненавистнического содержания, материалами суицидальной направленности, сектантскими материалами, ненормативной лексикой. Такую информацию относят к материалам нежелательного характера. Если порнографические материалы или материалы с ненормативной лексикой можно относительно легко идентифицировать и отсечь с помощью средств фильтрации, то от нежелательных материалов других типов детей защитить гораздо сложнее.

Например, на детских сайтах могут встречаться самые разные формы выражения ненависти: от радикального расизма до грубого высмеивания. Такие сайты на первый взгляд могут казаться безобидными, но они вносят свой вклад в формирование детской онлайновой культуры, в которой грубость по отношению к другим считается допустимой. Расисты и группы ненависти стали использовать Интернет для привлечения молодежи в свои ряды. Последние ищут восприимчивых молодых людей, а затем вовлекают их в свое сообщество, используя для этого чаты и электронную почту.

Некоторые ненавистнические сайты создают разделы специально для детей. Эта часть сервера специально имеет располагающий вид, предлагает безобидные игровые занятия и дает ссылки на уважаемые сайты.

КАК ПОМОЧЬ СВОИМ ДЕТЯМ ИЗБЕЖАТЬ НЕНАВИСТНИЧЕСКИХ МАТЕРИАЛОВ?

Используйте средства фильтрации нежелательного. Но фильтры могут только помочь в блокировании некоторых нежелательных материалов, они не могут полностью решить проблему. Выражения ненависти, встречающиеся в Интернете, часто принимают мягкие формы и не всегда распознаются фильтрами. Поэтому важно поддерживать доверительные отношения с детьми, чтобы они без колебаний обращались к вам за помощью. Контролируйте использование Интернета и наблюдайте за детьми. Как правило, дети, не достигшие десятилетнего возраста, еще не имеют навыков критического мышления, необходимого для самостоятельного посещения Сети. Расскажите детям о существующих в Интернете способах выражения ненависти. Научите их распознавать материалы с ненавистническим содержанием и символикой, например, изображение свастики, оскорбительные отзывы о расовой принадлежности, карикатурные описания разных этнических и расовых групп. Вашим детям будет легче избежать материалов ненавистнического содержания, если они будут знать об истории расизма, шовинизма и стратегиях распространителей ненависти. Младшим детям нужно подробно объяснить, что это за материалы, для чего их публикуют, какие опасности они несут, в чем состоит вред расовых концепций.

Старших детей необходимо научить критически относиться к содержанию онлайновых материалов и не доверять им без совета с вами.

ВОЗРАСТНЫЕ ОСОБЕННОСТИ ДЕТЕЙ И ИНТЕРНЕТ

Ребенок проходит в своем психологическом развитии определенные стадии, которые достаточно сильно отличаются друг от друга. Это также отражается и на интересах детей при работе в Интернете. Родителям важно знать, какие особенности имеют дети в том или ином возрасте, для того чтобы правильно расставлять акценты внимания при своих беседах с детьми о правилах безопасности в Интернете. Кроме того, нужно учитывать, что наши дети начинают осваивать Интернет в разном возрасте: кто-то в возрасте 14 - 17 лет, находясь в старших классах, кто-то в 10 - 13 лет, а кто-то еще в дошкольном возрасте получает первый опыт взаимодействия с Интернетом.

ДЕТИ В ВОЗРАСТЕ ДО 7 ЛЕТ И ИНТЕРНЕТ

Последние проведенные исследования показали, что дошкольники являются наиболее быстрорастущим сегментом пользователей Сети. Хотя дети в этом возрасте уделяют Интернету немного внимания, онлайновые изображения и звуки могут стимулировать воображение и развивать их фантазию.

Они могут получить доступ к развивающим играм и материалам, размещенным в Интернете, что будет стимулировать их интеллектуальное развитие.

ЧТО ДЕТИ ДО 7 ЛЕТ ОБЫЧНО ДЕЛАЮТ В ИНТЕРНЕТЕ?

На этом этапе деятельность детей в Интернете должна проходить при активном участии родителей. Взрослые могут посадить ребенка к себе на колени во время просмотра семейных фотографий, использования веб-камеры для общения с родственниками или посещения детских сайтов. У детей этого возраста обычно открытая натура и положительный взгляд на мир. Они гордятся приобретенными начальными умениями читать и считать и любят делиться идеями. Они не только хотят вести себя хорошо, но и доверяют авторитетам и редко в них сомневаются. Дети в этом возрасте, как правило, легко осваивают Интернет, обучаются основным навыкам при работе с ним. И хотя дошкольники могут быть очень способными в играх, выполнении команд на компьютере и работе с мышью, они сильно зависят от взрослых при поиске сайтов, интерпретации информации из Интернета или отправке электронной почты. Взрослые играют ключевую роль в обучении детей в этом возрасте безопасному использованию Интернета. Поэтому используйте это время для того, чтобы сформировать у своего ребенка культуру безопасной работы в Интернете.

Дети этого возраста должны выходить в Интернет только под присмотром родителей.

ДЕТИ В ВОЗРАСТЕ ОТ 7 ДО 10 лет ИИНТЕРНЕТ (МЛАДШИЙ ШКОЛЬНЫЙ ВОЗРАСТ)

Семи-десятилетние дети обладают сильным чувством семьи. Они только начинают развивать чувство своей моральной и половой индивидуальности и обычно интересуются жизнью старших детей. Они доверчивы и не сомневаются в авторитетах. Как правило, дети, не достигшие десятилетнего возраста, еще не имеют навыков критического мышления, необходимого для адекватного осмысления материалов, встречающихся в Интернете.

Дети этого возраста начинают активно самостоятельно осваивать виртуальное пространство, любят путешествовать по Интернету, играть в сетевые игры, они начинают общаться в детских чатах, стремятся использовать электронную почту для переписки с друзьями. Однако нужно иметь в виду, что они могут заходить на сайты и чаты, посещать которые родители им не разрешали.

Старайтесь держать компьютеры с подключением к Интернету в общих комнатах, в которых можно легко осуществлять визуальный контроль над тем, что делает ваш ребенок в Интернете. Создайте при участии детей свод домашних правил пользования Интернетом и требуйте его неукоснительного соблюдения. Приучите детей посещать только те сайты, которые вы разрешили.

Используйте средства блокирования нежелательного материала. Используйте фильтры электронной почты для блокирования сообщений от конкретных людей или содержащих определенные слова или фразы.

Создайте семейный электронный ящик, на который будет приходить вся ваша электронная почта, вместо того чтобы позволять детям иметь собственные адреса. Научите детей советоваться с вами перед раскрытием информации через электронную почту, чаты, доски объявлений, регистрационные формы и личные профили. Научите детей не загружать программы, музыку или файлы без вашего разрешения. Позволяйте детям заходить на детские сайты только с хорошей репутацией и контролируемым общением. Не разрешайте детям этого возраста пользоваться службами мгновенного обмена сообщениями. Беседуйте с детьми об их друзьях в Интернете и о том, чем они занимаются так, как если бы речь шла о друзьях в реальной жизни. Приучите детей сообщать вам, если что-либо или кто- либо в Сети тревожит или угрожает им. Оставайтесь спокойными и напомните детям, что они в безопасности, если рассказали вам. Похвалите их и побуждайте подойти еще раз, если случай повторится.

ДЕТИ В ВОЗРАСТЕ ОТ 10 ДО 13 ЛЕТ И ИНТЕРНЕТ

10 - 13 лет - младший подростковый и средний школьный возраст - время быстрых изменений в жизни вашего ребенка. И хотя дети в этом возрасте все еще сильно зависимы от своих родителей, они уже стремятся получить некоторую свободу действий. Ребята начинают интересоваться миром вокруг них, и отношения с друзьями становятся по-настоящему важными.

Дети этого возраста начинают использовать Интернет для разработки школьных проектов. Кроме того, они загружают музыку, пользуются электронной почтой, играют в онлайновые игры и заходят на фанатские сайты своих кумиров.

Все более часто их любимым способом общения становится мгновенный обмен сообщениями. Для детей этого возраста желание выяснить, что они могут себе позволить делать без разрешения взрослых, является абсолютно нормальным. Находясь в Интернете, ребенок может попытаться посетить сайты или пообщаться в чатах, разрешения на которые он не получил бы от родителей. Отчеты о деятельности в Интернете от сервиса MSN Premium или других служб могут быть особенно полезными на этом этапе. У детей не будет ощущения, что родители постоянно смотрят на экран через их плечо; однако благодаря отчетам взрослые будут по-прежнему знать, какие сайты посещают их дети.

Убедитесь в том, что ваш ребенок знает и выполняет правила поведения для детей более раннего возраста, если он только начинает пользоваться Интернетом. Создайте ребенку собственную учетную запись с ограниченными правами, чтобы он не мог заниматься чем-то посторонним без вашего ведома.

Создайте при участии подростков и поддерживайте соблюдение списка домашних правил при работе в Интернете. Следует указать список сайтов, запрещенных для посещения, часы нахождения в Сети и руководство по общению в Интернете (в том числе и в чатах).

Используйте средства фильтрования нежелательного материала как дополнение, но не замену к родительскому контролю. Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету без вашего присутствия.

Требуйте от детей никогда не выдавать личную информацию, в том числе фамилию, имя, домашний адрес, номера телефонов, название школы, адрес электронной почты, фамилии друзей или родственников, свои имена в программах мгновенного обмена сообщениями, возраст или дату рождения, по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете.

Требуйте от детей не загружать из Интернета программы без вашего разрешения. Кроме того, объясните детям, что, делая файлы общими или загружая из Интернета тексты, фотографии или рисунки, они могут нарушать чьи-то авторские права.

Приучите детей сообщать вам, если что-либо или кто-либо в Сети тревожит или угрожает им. Оставайтесь спокойными и напомните детям, что они в безопасности, поскольку рассказали вам о новых угрозах. Похвалите их и побуждайте подойти еще раз, если случай повторится. Настаивайте на том, чтобы дети предоставили вам доступ к своей электронной почте, чтобы вы могли убедиться, что они не общаются с незнакомцами. Контроль лучше всего осуществлять ненавязчиво, уважая личное достоинство и право ребенка на самостоятельность. Расскажите детям об ответственном, достойном поведении в Интернете. Ребята ни в коем случае не должны использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

ДЕТИ В ВОЗРАСТЕ 14 - 17 ЛЕТ И ИНТЕРНЕТ

Подростки, как правило, проходят через период низкой самооценки; ищут поддержку у друзей и неохотно слушаются родителей. Более старшие ищут свое место в мире и пытаются обрести собственную независимость; в то же время они охотно приобщаются к семейным ценностям. В этом возрасте подростки уже полноценно общаются с окружающим миром. Они бурлят новыми мыслями и идеями, но испытывают недостаток жизненного опыта. Родителям важно продолжать следить, как используют Интернет их дети в этом возрасте.

В этом возрасте дети уже наслышаны о том, какая информация существует в Интернете. И совершенно нормально, что они хотят все это сами увидеть, услышать, прочесть. Доступ к нежелательным материалам (например, порнографическим картинкам или инструкциям по изготовлению взрывчатки) можно легко заблокировать при помощи программных фильтров. Они скачивают музыку, пользуются электронной почтой, службами мгновенного обмена сообщениями и играют. Кроме того, подростки активно используют поисковые машины. Большинство пользовалось чатами, и многие общались в приватном режиме. Мальчики в этом возрасте склонны сметать

все ограничения и жаждут грубого юмора, крови, азартных игр и картинок для дамы более чувствительны к сексуальным домогательствам в Интернете.

Сетевая безопасность подростков - трудная задача, поскольку об Интернете они знают зачастую больше, чем их родители. Тем не менее участие взрослых тоже необходимо. Особенно важно строго соблюдать правила Интернет-безопасности - соглашение между родителями и ребенком. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернете. Родители должны также помнить о необходимости хранить свои пароли в секрете, чтобы подростки не смогли зарегистрироваться под именем старших.

Измените в соответствии с интересами и запросами подростка список домашних правил использования подростком Интернета, требуйте его соблюдения. Беседуйте с подростками об их друзьях в Интернете и о том, чем они занимаются. Спрашивайте о людях, с которыми подростки общаются по мгновенному обмену сообщениями, и убедитесь, что эти люди им знакомы.

Интересуйтесь, какими чатами и досками объявлений пользуются подростки и с кем они общаются. Поощряйте использование модерируемых чатов и настаивайте, чтобы они не общались с кем-то в приватном режиме. Возьмите за правило знакомиться с сайтами, которые посещают ваши дети. Убедитесь, что они не посещают сайты с оскорбительным содержанием, не публикуют личную информацию или свои фотографии. Настаивайте, чтобы подростки никогда не соглашались на личные встречи с друзьями из Интернета без вашего участия. Напоминайте, какие опасности это может за собой повлечь. Требуйте от подростков никогда не выдавать личную информацию по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете. Напоминайте, чем это может обернуться.

Требуйте от подростков не загружать программы, музыку или файлы без консультаций с вами. Объясните, что иначе подростки могут нарушить авторские права и тем самым закон. Настаивайте на том, чтобы подростки ставили вас в известность, если что-либо или кто-либо в Сети тревожит или угрожает им. Объясните, что угрозы им - это также и угроза всей семье. Оставайтесь в случае чего спокойными и напомните детям, что они в безопасности, если рассказали вам. Помогайте им решить возникшие проблемы.

Помогайте им защититься от спама. Научите подростков не выдавать в Интернете своего электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры. Постоянно напоминайте, что ребята ни в коем случае не должны использовать Сеть для хулиганства, распространения сплетен или угроз другим людям. Убедитесь, что подростки советуются с вами перед покупкой или продажей чего-либо в Интернете. Обсудите с подростками азартные сетевые игры и связанный с ними риск. Напомните, что детям нельзя в них играть. Поддерживайте уровень

безопасности вашего компьютера на должном уровне. Если ваш ребенок лучше вас разбирается в программном обеспечении, то почему бы не поручить ему заботу о безопасности ваших семейных компьютеров?

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ:

Повысьте меры компьютерной защиты до максимально приемлемого уровня на компьютере, который ваш ребенок предполагает использовать вне дома. Особое внимание обратите политике конфиденциальности. Для этого можно воспользоваться мерами, которые описаны в соответствующем разделе данной брошюры. Установите надежный пароль. Пароль защищает компьютер и блокирует возможность его использования без разрешения его владельца. Напомните вашему ребенку, что ему нельзя сообщать этот пароль своим друзьям, а если он стал им известен, то пароль должен быть изменен.

Пароли являются первой линией защиты от злоумышленников, шутников или беспечного соседа по комнате. Если вы не пользуетесь паролем для входа в компьютер, кто угодно может получить доступ. Требуйте от детей всегда блокировать доступ к компьютерной системе на то время, когда он с ней не работает.

Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры. Постоянно напоминайте, что ребята ни в коем случае не должны использовать Сеть для хулиганства, распространения сплетен или угроз другим людям. Убедитесь, что подростки советуются с вами перед покупкой или продажей чего-либо в Интернете. Обсудите с подростками азартные сетевые игры и связанный с ними риск. Напомните, что детям нельзя в них играть. Поддерживайте уровень безопасности вашего компьютера на должном уровне. Если ваш ребенок лучше вас разбирается в программном обеспечении, то почему бы не поручить ему заботу о безопасности ваших семейных компьютеров?

РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ:

Повысьте меры компьютерной защиты до максимально приемлемого уровня на компьютере, который ваш ребенок предполагает использовать вне дома. Особое внимание обратите политике конфиденциальности. Для этого можно воспользоваться мерами, которые описаны в соответствующем разделе данной брошюры. Установите надежный пароль. Пароль защищает компьютер и блокирует возможность его использования без разрешения его владельца. Напомните вашему ребенку, что ему нельзя сообщать этот пароль своим друзьям, а если он стал им известен, то пароль должен быть изменен.

Пароли являются первой линией защиты от злоумышленников, шутников или беспечного соседа по комнате. Если вы не пользуетесь паролем для входа в компьютер, кто угодно может получить доступ. Требуйте от детей всегда блокировать доступ к компьютерной системе на то время, когда он с ней не работает.

Лекция для учащихся.

Мы все общаемся в Интернете. Так же часто, как и в коридорах школы, во дворе или на улице. Вообще Интернет - это отличная вещь для общения с тем, кто находится далеко от тебя. В Сети легко выкладывать видео, музыку, рассказывать о себе, разговаривать и спорить. Удобно находить новых друзей, устраивать с ними новые развлечения и игры.

Но мы все всегда хотим, чтобы общаться нам было комфортно. Комфортно - это значит, чтобы общение нас не «напрягало», чтобы мы не боялись находиться в какой-нибудь компании, чтобы нам там не было неловко. И уж, конечно, чтобы не попадать в неприятные ситуации. Не говоря уже о том, чтобы на каждого из нас не «наезжали», не обзывали и не дразнили.

К сожалению, в Интернете гораздо легче попасть в такую неприятную ситуацию или нарваться на хама, чем на улице. Те, кто ведет себя в Сети неподобающим образом, забывают, что Интернет - это вовсе не место для хамства, унижений или неуместных шуток. И безопасный Интернет, позитивный Интернет - это в первую очередь такой Интернет, в котором ничего подобного нет, а хамы и тролли немедленно наказываются.

Чаще всего мы в Интернете общаемся словесно. Иногда с кем-то вдвоем (например, в чате или мгновенном мессенджере типа Skype), но чаще - как на лавочке во дворе, целой компанией. Обычно это бывает на форуме - специальном онлайн-ресурсе, созданном для общения. Разновидностью форумов являются функции комментариев к постам в соцсети, в блогах или под какой-нибудь статьей в онлайн-газете.

Часто бывает, что чьи-то точки зрения не сошлись. Спорят, спорят... И кто-то вдруг начинает хамить. Обзывать собеседника (или всех разом), дразнить, высмеивать его внешность, одежду, родителей. Тот, кого обозвали, может какое-то время держаться, но обычно очень быстро тоже «срывается». И все - в теме начинается «словесная драка». Причем она очень долго не затихает, и зачастую в ход идут «запрещенные» приемы - те, которые мы никогда не используем в оффлайновойтусовке.

А почему так происходит? Или спросим по-другому: почему в Интернете все происходит более жестко, чем в оффлайне? Для этого есть несколько причин.

Очень часто юзеры считают, что в Интернете все «не всерьез».

Дескать, мы же не вживую общаемся. А если речь идет о чате в какой-нибудь игре, так это вообще мой эльф беседует с каким-то гоблином или драконом. Интернет-игра - это свой мир, а лавочка во дворе - свой... Ведь пишут же в газетах про «**виртуальный мир**»?

На самом деле такие юзеры неправы. Какого-то отдельного «**виртуального мира**», «**мира в Интернете**» нет и никогда не было. Компьютер - это всего лишь устройство, как телевизор или плеер. И все, что мы за ним делаем - мы делаем в реальном мире. В том числе и на лавочке во дворе. Что значит - беседуем мы не с мифическими эльфами или драконами, а с такими же людьми, хоть мы их и не видим.

Некоторые юные юзеры ведут себя иначе в Интернете как раз потому, что собеседники их не видят. Они считают, что они таким образом полностью анонимны - как в «шапке-невидимке», которой нет на улице. А значит, обиженный собеседник не сможет поймать обидчика «в темном уголке». И в этом они тоже неправы. Интернет далеко не анонимен, и есть множество способов узнать, с кем вы разговаривали на таком-то сайте. Некоторые способы простые, некоторые - посложнее, но все они работают. И наказание за те или иные действия в Интернете вполне может наступить.

А самое главное - **в Сети все, что было «сказано» - написано, остается надолго.** Сказанные слова легко потерять и забыть, а вот написанные - нет. Поэтому даже спустя годы некто может увидеть, как некрасиво вел себя некий юзер когда-то. И вот об этом тоже неплохо помнить, беседуя с незнакомцами в Сети. Зато культурное общение будет «работать» уже в твою пользу - опять же спустя годы, потому что все смогут убедиться в твоей культурности.

В Сети есть свои правила поведения - **Нетикет**, то есть «**сетевой этикет**». На самом деле эти правила ничем не отличаются от правил хорошего поведения на улице - потому что, когда мы сидим за компьютером, мы и есть на улице. Но есть среди них один главный закон. Его придумал один немецкий философ за много лет до Интернета. Он гласит: «Поступай с другими так же, как ты хочешь, чтобы поступали с тобой». Может, действительно будет нелишним «примерить» каждый поступок в Сети на себя - и тогда будет понятнее, надо ли сделать что-то или нет?

НЕЗНАКОМЕЦ или ДРУГ?

Блоги и социальные сети помогают нам искать друзей. Даже заводить новых. Это называется «**френдить**» или «**зафренживать**» - от английского слова, которое значит «друг». Но почему было бы просто не сказать «заводить друзей» или «подружиться»?

А потому что создатели этих словечек знали, что друг в школе или во дворе и «френд» в Интернете - это «две большие разницы». Друга в оффлайне каждый из нас знает в лицо. «Постойте», - скажете вы, - «но в Интернете френда мы тоже знаем в лицо. Вон его фотография в аватаре...» А Вы уверены, что это его фотография? Живьем-то мы нашего френда в Сети обычно не видим. И поэтому за этой фотографией или картинкой может скрываться кто угодно. Вместо мальчика - девочка, вместо первоклассника - десятиклассник, и вообще вместо девочки - дедушка.

Так что никогда нельзя быть стопроцентно уверенным в том, что с тобой в Сети разговаривает именно тот человек, кем он назвался. В конце концов, бывает и так, что одним аккаунтом пользуются два человека, а то и больше. Именно поэтому к Интернет-знакомому надо **ВСЕГДА** относиться как к незнакомцу. А это значит:

- Общаться вежливо, как в магазине или в автобусе;
- Ни в коем случае не провоцировать на грубость и не грубить самому;
- Не рассказывать свои секреты и тем более секреты родителей или других взрослых! Очень часто бывает так, что кто-то втирается в доверие через

Интернет, узнает много личного и затем планирует преступление - в отношении тебя, твоих родителей, близких.

Конечно, все это не относится к тем случаям, для которых блоги и социальные сети и делались - то есть когда ты общаешься с теми, кого ты знаешь по школе, по двору или по спортивной секции. Но все равно можно лишний раз уточнить у своего друга или подруги, действительно ли он\она ведет эту страничку - или это делает кто-то чужой, прикрываясь знакомой фотографией? И, кстати, даже с хорошо знакомыми друзьями лучше не доверять тайны Интернету. А вдруг онлайн-переписку взломает хакер?

ТРОЛЛИ

Но бывают и такие, для кого похамить в Интернете - главное и любимое занятие. Они специально ищут такие места в Сети, где общается много людей. Выбирают там одного юзера - и начинают его травить. Иногда это делает кто-то один, иногда этим начинает заниматься целая группа. А бывает и так, что один юзер заводит себе несколько аккаунтов - создается впечатление, что травлей занимается несколько человек... И часто бывает так: кто-то один начал травить кого-то - в это дело начинают включаться другие юзеры, и вместо нормальной беседы начинается ужас.

Как вы уже знаете, таких юзеров называют «**тролли**». Тролли говорят, что они делают беседу более «правильной» и более веселой. На самом деле это не так, и они сами знают, что это не так. Вот когда они говорят, что «задирать» кого-то в Сети безопасней, чем на улице - они говорят более честно. Действительно, они думают, что в Интернете они анонимны, «велики и ужасны». В обычной же жизни они всегда боятся, что за такое поведение им кто-то обязательно отвесит подзатыльник - поэтому они и идут в Сеть, где будто бы «безопасней». Как правило, в обычной жизни тролль ничего из себя не представляет - и об этом качестве троллей знают все. Так что лучше не идти их дорогой, а то будут тоже воспринимать за неудачника...

Спорить с троллем бесполезно. Он будет находить все новые и новые вещи, за которые можно «зацепиться». Платить ему той же монетой, то есть хамить в ответ? Да ему этого и надо! Ему нужно доказать - другим и себе - что на этом форуме или в блоге есть кто-то еще хуже, чем он сам. А самая главная цель - чтобы пришел модератор и забанил того, кого он травил, а не его самого. Можно, конечно, постараться высмеять самого **тролля**, но **тролль** - существо очень упорное, просто так не отвяжется, потому что отвязаться для него - самое страшное. Да и от насмешки до хамства недалеко - не заметишь, как перейдешь эту границу.

Лучше всего, когда на сайте собрались такие юзеры, которые не любят троллей. Они просто не будут обращать внимания на любые попытки тролля кому-то нахамить и «выключат» его из общения. Но чаще всего это всего лишь мечта. Тогда. На каждом ресурсе есть модератор - как бы он ни назывался. Проще говоря, тот, кто наводит порядок на данной страничке. Можно отправить личное сообщение ему - он примет меры к троллю. Ведь это и в его интересах - ему же хочется, чтобы его страничка была удобной для юзеров. Но бывает и так, когда модератор сам на стороне тролля. Тогда лучше с такого

ресурса уйти. Ничего «позорного» в этом нет - ведь бороться можно только по правилам. А похожих ресурсов в Интернете море - и там окажется также интересно и полезно, да к тому же и более безопасно.

Если тролль пишет тебе в электронную почту или в мгновенный мессенджер - все проще: нужно просто внести его в «**черный список**». Тогда сообщения от этого юзера перестанут тебе приходить.

КИБЕРУНИЖЕНИЕ

На видеохостингах и в социальных сетях нередко можно встретить такие видеоролики, когда группа мальчиков и девочек издеваются над другим мальчиком или девочкой, дразнят их, обзывают, заставляют проделывать унизительные вещи, а то и бьют. Иногда на месте такого мальчика или девочки может оказаться взрослый, например старый человек... Наверное, это самое плохое, что только можно додуматься выложить в Интернет.

Зачем это делается? Некоторым глупым ребятам кажется, что это весело и забавно. А еще им очень хочется показать, что они «круче» и сильнее, чем на самом деле. Особенно когда их много - ведь в одиночку они бы это делать наверняка побоялись, ведь так поступают только трусы. Иногда им даже кажется, что они так справедливо мстят - например, за какое-то неосторожное слово, которое им сказали. Они ждут, что все посмотрят это видео и скажут: «Вот какие классные ребята! Они весело проводят время, с ними надо дружить». Или: «Ой, какие они сильные! Их надо бояться».

На самом деле это не так. Большинство нормальных людей оставляют под такими видео каменты совершенно другого плана. «Какие дураки!», «Трусы», «Зверьки», а то и «Надо сообщить в полицию». И сообщают! А это значит - серьезные проблемы у тех, кто кажется таким смелым на видео. Думаете, если человеку еще нет 16, то ему ничего от полиции не будет? Серьезно ошибаетесь! Да и потом, лет через десять-двадцать, увидят такое видео будущие коллеги по работе или взрослые друзья и... Поскольку они уже взрослые, скорее всего отвернутся от такого «друга» - потому что им будет за него стыдно. Кстати, «веселым ребятам» потом будет сложнее найти работу, среди всего прочего. Может быть, лучше помнить старую пословицу «Береги честь смолоду»?

Если вам попалось такое видео в Интернете - нужно тут же сообщить о нем модератору или в полицию, которая борется с таким контентом. Видео с каментами тут же заблокируют.

Язык ненависти.

Как уже говорилось, за хамство в Интернете принято наказывать. Но если кто-то думает, что для этого нужно оскорбить обязательно какого-то конкретного человека, то он сильно ошибается. Оскорбить можно и большую группу людей, никого конкретно из них по имени не называя...

Чаще всего в Интернете встречаются оскорбления и унижения по признакам принадлежности людей к определенной расе, национальности, религии, субкультуре. Иногда их авторы выражаются чересчур вычурно, иногда - очень просто, но суть одна: дескать, вот такие-то - плохие, неполноценные, не имеют права на собственное мнение или вообще ни на что.

Просто потому, что они вот такой национальности, там- то родились или фанатеют от таких-то исполнителей.

Подобные посты принято называть очень просто: «Язык Ненависти». Потому что он несет в себе ненависть и вражду. А может и провоцировать на силовые действия в отношении тех или иных людей - такое тоже нередко.

Наверное, излишне говорить, что считать людей «неполноценными» или «плохими» только потому, что они имеют другой цвет кожи, жи вут в другом городе или стране, или болеют за другой клуб, просто глупо. История человечества многократно доказывала, что никакой разницы между людьми в этом плане нет, а уж что касается их увлечений и взглядов, то это вообще дело каждого. Любители «языка ненависти» часто не думают, что ведь кому-то и их увлечение может казаться глупым - при том, что «наехать» на этого «кого-то» ну никак не получится: он развит и успешен, так что к «неполноценным» его отнести никак не получится.

В Интернете «язык ненависти» звучит чаще всего в двух случаях: если кто-то хочет «казаться своим» или если кто-то проигрывает спор. Встретить его можно практически на всех типах онлайн-площадок, где люди общаются: от чатов и форумов до социальных сетей. Правда, встретить его можно только до тех пор, пока до такого поста не дотянулся модератор.

И хорошо, если только модератор. «Язык ненависти» - одно из самых серьезных преступлений, которые встречаются в Интернете. Юристы называют его «разжигание межнациональной и религиозной розни» - это преступление в разных странах рассматривается как преступление против личности, против государства, а то и против человечества (например, в Беларуси). Естественно, что наказание за «язык ненависти» в Интернете следует быстро и неотвратимо - и в отношении тех, кто позволяет себе такой «язык», и в отношении сайтов, на которых - при попустительстве модераторов - он процветает.

Памятка для родителей об информационной безопасности детей

Определение термина «информационная безопасность детей» содержится в Федеральном законе № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», регулирующим отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию. Согласно данному закону «информационная безопасность детей» - это состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию. В силу Федерального закона № 436-ФЗ информацией, причиняющей вред здоровью и (или) развитию детей, является:

1. информация, запрещенная для распространения среди детей;
2. информация, распространение которой ограничено среди детей определенных возрастных категорий.

К информации, запрещенной для распространения среди детей, относится:

1. информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в т.ч. причинению вреда своему здоровью, самоубийству;
2. способность вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе; принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
3. обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям и животным;
4. отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
5. оправдывающая противоправное поведение;
6. содержащая нецензурную брань;
7. содержащая информацию порнографического характера.

К информации, распространение которой ограничено среди детей определенного возраста, относится:

1. информация, представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;
2. вызывающая у детей страх, ужас или панику, в т.ч. представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;
3. представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;
4. содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

С учетом этого Вам предлагаются правила работы в сети Интернет для различных возрастных категорий, соблюдение которых позволит обеспечить информационную безопасность ваших детей.

Общие права для родителей

1. Независимо от возраста ребенка используйте программное обеспечение, помогающее фильтровать и контролировать информацию, но не полагайтесь полностью на него. Ваше внимание к ребенку - главный метод защиты.
2. Если Ваш ребенок имеет аккаунт на одном из социальных сервисов (LiveJoumal, blogs.mail.ru, vkontakte.ru и т.п.), внимательно изучите, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео.
3. Проверьте, с какими другими сайтами связан социальный сервис Вашего ребенка. Странички Вашего ребенка могут быть безопасными, но могут и содержать ссылки на нежелательные и опасные сайты (например, порносайт, или сайт, на котором друг упоминает номер сотового телефона Вашего ребенка или Ваш домашний адрес)
4. Поощряйте Ваших детей сообщать обо всем странном или отталкивающим и не слишком остро реагируйте, когда они это делают (из-за опасения потерять доступ к Интернету дети не говорят родителям о проблемах, а также могут начать использовать Интернет вне дома и школы).
5. Будьте в курсе сетевой жизни Вашего ребенка. Интересуйтесь, кто их друзья в Интернет так же, как интересуетесь реальными друзьями.

Возраст от 7 до 8 лет

В Интернете ребенок старается посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям особенно полезны будут те отчеты, которые предоставляются программами по ограничению использования Интернета, т. е. Родительский контроль или то, что вы сможете увидеть во временных файлах. В результате, у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако, родители будут по-прежнему знать, какие сайты посещает их ребенок. Дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Они любят играть в сетевые игры и путешествовать по Интернету, используя электронную почту, заходить на сайты и чаты, не рекомендованные родителями.

Советы по безопасности в сети Интернет для детей 7-8 лет

1. Создайте список домашних правил посещения Интернета при участии детей и требуйте его выполнения.
2. Требуйте от Вашего ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что Вы наблюдаете за ним не потому что Вам это хочется, а потому что Вы беспокоитесь о его безопасности и всегда готовы ему помочь.
3. Компьютер с подключением к Интернету должен находиться в общей комнате под присмотром родителей.
4. Используйте специальные детские поисковые машины.
5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
6. Создайте семейный электронный ящик, чтобы не позволить детям иметь

собственные адреса.

7. Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего программного обеспечения.

8. Приучите детей советоваться с Вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.

9. Научите детей не загружать файлы, программы или музыку без вашего согласия.

10. Не разрешайте детям использовать службы мгновенного обмена сообщениями.

11. В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.

12. Не забывайте беседовать с детьми об их друзьях в Интернете, как если бы речь шла о друзьях в реальной жизни.

13. Не делайте «табу» из вопросов половой жизни, так как в Интернете дети могут легко наткнуться на порнографию или сайты «для взрослых».

14. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Возраст детей от 9 до 12 лет

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернете. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

Советы по безопасности для детей от 9 до 12 лет

1. Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.

2. Требуйте от Вашего ребенка соблюдения норм нахождения за компьютером.

3. Наблюдайте за ребенком при работе за компьютером, покажите ему, что Вы беспокоитесь о его безопасности и всегда готовы оказать ему помощь.

4. Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.

5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

6. Не забывайте принимать непосредственное участие в жизни ребенка беседовать с детьми об их друзьях в Интернете.

7. Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.

8. Позволяйте детям заходить только на сайты из «белого» списка, который создайте вместе с ними.

9. Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями,

регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.

10. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

11. Создайте Вашему ребенку ограниченную учетную запись для работы на компьютере.

12. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах и опасениях.

13. Расскажите детям о порнографии в Интернете.

14. Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.

15. Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок «для взрослых». Девочки предпочитают общаться в чатах, при этом они гораздо более чувствительны к сексуальным домогательствам в Интернете.

Зачастую в данном возрасте родителям уже весьма сложно контролировать своих детей, так как об Интернете они уже знают значительно больше своих родителей. Тем не менее, не отпускайте детей в «свободное плавание» по Интернету. Старайтесь активно участвовать в общении ребенка в Интернете.

Важно по-прежнему строго соблюдать правила Интернет-безопасности - соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернете. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

Советы по безопасности в этом возрасте от 13 до 17 лет

1. Создайте список домашних правил посещения Интернета при участии подростков и требуйте безусловного его выполнения. Обговорите с ребенком список запрещенных сайтов («черный список»), часы работы в Интернете, руководство по общению в Интернете (в том числе в чатах).

2. Компьютер с подключением к сети Интернет должен находиться в общей комнате.

3. Не забывайте беседовать с детьми об их друзьях в Интернете, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.

4. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

5. Необходимо знать, какими чатами пользуются Ваши дети. Поощряйте

использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.

6. Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.

7. Приучите детей не выдавать свою личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.

8. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

9. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам, о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

10. Расскажите детям о порнографии в Интернете. Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего реального

электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

11. Приучите себя знакомиться с сайтами, которые посещают подростки.

12. Научите детей уважать других в интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде — даже в виртуальном мире.

13. Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

14. Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

Постоянно контролируйте использование Интернета Вашим ребенком! Это не нарушение его личного пространства, а мера предосторожности и проявление Вашей родительской ответственности и заботы.

ПАМЯТКА ДЛЯ УЧАЩИХСЯ

ОБЩИЕ ПРАВИЛА ИНТЕРНЕТА

Важно помнить, что в Интернете есть свои правила и границы, свои «НЕЛЬЗЯ!», «ОСТОРОЖНО!», МОЖНО!»:

НЕЛЬЗЯ!

1. Всем подряд сообщать свою частную информацию (настоящие имя, фамилию, телефон, адрес, номер школы, а также фотографии свои, своей семьи и друзей).
2. Открывать вложенные файлы электронной почты, когда не знаешь отправителя.
3. Грубить, придираться, оказывать давление — вести себя невежливо и агрессивно.
4. Не распоряжайся деньгами твоей семьи без разрешения старших - всегда спрашивай родителей;
5. Не встречайся с Интернет-знакомыми в реальной жизни - посоветуйся со взрослым, которому доверяешь.

ОСТОРОЖНО!

1. Не все пишут правду. Читаешь о себе неправду в Интернете — сообщи об этом своим родителям или опекунам.
2. Приглашают переписываться, играть, обмениваться - проверь, нет ли подвоха.
3. Незаконное копирование файлов в Интернете – воровство.
4. Всегда рассказывай взрослым о проблемах в сети - они всегда помогут.
5. Используй настройки безопасности и приватности, чтобы не потерять свои аккаунты в соцсетях и других порталах.

МОЖНО!

1. Уважай других пользователей.
2. Пользуешься Интернет-источником - делай ссылку на него.
3. Открывай только те ссылки, в которых уверен.
4. Общаться за помощью взрослым - родители, опекуны и администрация сайтов всегда помогут.

БЕЗОПАСНОЕ ПОВЕДЕНИЕ В ИНТЕРНЕТЕ

С каждым годом молодежи в интернете становиться больше, а школьники одни из самых активных пользователей Рунета. Между тем, помимо огромного количества возможностей, интернет несет и проблемы. Эта памятка должна помочь тебе безопасно находиться в сети.

КОМПЬЮТЕНРЫЕ ВИРУСЫ

Компьютерный вирус - это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена заражённая программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

Методы защиты от вредоносных программ:

1. Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ.
2. Постоянно устанавливай патчи (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его.
3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;
4. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
5. Ограничь физический доступ к компьютеру для посторонних лиц;
6. Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;
7. Не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

СОЦИАЛЬНЫЕ СЕТИ

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей.
2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы.
3. Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить.

4. Избегай групп и пользователей, говорящих на языке насилия и ненависти, призывающих к тем действиям, которые никогда бы не одобрили твои родители.

5. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее.

6. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение.

7. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8.

8. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

ЭЛЕКТРОННАЯ ПОЧТА

Электронная почта — это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя_пользователя@имя_домена. Также кроме передачи простого текста, имеется возможность передавать файлы.

Основные советы по безопасной работе с электронной почтой:

1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге.

2. Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный_фанат@» или «рок2013» вместо «тема13».

3. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль.

4. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;

5. Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;

6. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».

КИБЕРБУЛЛИНГ

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернетсервисов.

Основные советы по борьбе с кибербуллингом:

1. Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше

разожжешь конфликт.

2. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом.

3. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно.

4. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии.

5. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов.

6. Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

ОНЛАЙН ИГРЫ

Современные онлайн-игры - это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции.

Все эти средства идут на поддержание и развитие игры, а также на саму безопасность: совершенствуются системы авторизации, выпускаются новые патчи (цифровые заплатки для программ), закрываются уязвимости серверов.

В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.

Основные советы по безопасности твоего игрового аккаунта:

1. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков.

2. Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов.

3. Не указывай личную информацию в профайле игры.

4. Уважай других участников по игре.

5. Не устанавливай неофициальные патчи и моды.

6. Используй сложные и разные пароли.

7. Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

ЦИФРОВАЯ РЕПУТАЦИЯ

Цифровая репутация - это негативная или позитивная информация в сети о тебе. Компрометирующая информация размещенная в интернете может серьезным образом отразиться на твоей реальной жизни. «Цифровая

репутация» - это твой имидж, который формируется из информации о тебе в интернете.

Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких - все это накапливается в сети.

Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу. Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающее люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой - как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

Основные советы по защите цифровой репутации:

1. Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;
2. В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только «для друзей»;
3. Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.