Обеспечение медиабезопасности детей и подростков в сети Интернет

В современном мире мало кто задумывается о том, где найти ответ на тот или иной вопрос. Сотовые телефоны и всемирная сеть Интернет являются самыми распространенными средствами обмена идеями XX века, которые не только не прекратили своего стремительного роста, но и продолжают удерживать пальму первенства популярности. Интернет способен, с одной стороны, сделать жизнь человека комфортной, с другой - привести к беде. На основании этого стоит обратить внимание на такое понятие как «медиабезопасность».

Медиа - это обширное понятие, которое включает в себя всю совокупность средств и приемов, служащих для передачи информации человеку. Это могут быть:

– медиасредства массовой информации (телевидение, периодическая пресса, радио, кабельные телевизионные сети);

– директ медиа - коммуникационные системы передачи информации (интернет, телефон, почта);

– медианосители - отдельные носители информации (письма, записи на аудио- и видеоносителях, видео-, аудио-, презентации);

– социальные медиа - средства коммуникации групп сообществ между собой (социальные сети, блоги, персональные сайты, самиздатовская периодическая пресса).

Безопасность – это состояние защищённости. Защищённость от последствий воздействия на человека, а также защищённость жизненно важных интересов личности, общества, государства от потенциально и реально существующих угроз. Информационная безопасность детей - состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

Каждый человек, взрослый или ребенок, должен знать четкую грань между миром виртуальным и объективной реальностью, а государство старается защитить интересы

каждого человека и направить его деятельность в интернет-пространстве в нормативное русло. Особенно большое внимание уделяется безопасности детей. С этой целью создана целая *нормативная база* защиты детей от информации, которая причиняет вред их здоровью, репутации, нравственному, духовному и социальному развитию.

К таким документам относится:

1. Федеральный закон от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации», ст. 4, 37 Закона Российской Федерации от 27.12.1991 «О средствах массовой информации» № 2124-1.
2. Стратегия национальной безопасности Российской Федерации до 2020 года, утвержденной Указом Президента Российской Федерации от 12.05.2009 № 537.
3. Доктрина информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации 09.09.2000 № ПР-1895, в которой закреплены общие принципы обеспечения информационной безопасности граждан и государства.
4. Распоряжения Правительства РФ от 19.07.2006 № 1032-р и от 18.10.2007 № 1447-р, Письмо Министерства образования и науки Российской Федерации от 10.11.2006 № АС-1299/03 «О реализации контентной фильтрации доступа образовательных учреждений, подключаемых к сети Интернет в рамках приоритетного национального проекта «Образование».
5. Распоряжения Правительства РФ от 19.07.2006 № 1032-р и от 18.10.2007 № 1447-р, Письмо Министерства образования и науки Российской Федерации от 10.11.2006 № АС-1299/03 «О реализации контентной фильтрации доступа образовательных учреждений, подключаемых к сети Интернет в рамках приоритетного национального проекта «Образование».
6. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», который вступил в действие 01.09.2012.

Федеральный закон устанавливает правила медиабезопасности детей при распространении на территории России продукции средств массовой информации, печатной, аудиовизуальной продукции на любых видах носителей,

программ для ЭВМ и баз данных, а также информации, размещаемой в информационно-телекоммуникационных сетях и сетях радиотелефонной связи.

Закон содержит ряд инновационных норм, предусматривающих создание организационно-правовых механизмов защиты детей от распространения в сети Интернет вредной для них информации.

К информации, причиняющей вред здоровью и (или) развитию детей, законом отнесена информация, запрещенная для распространения среди детей, а также информация, распространение которой ограничено среди детей определенных возрастных категорий.

К информации, запрещенной для распространения среди детей, относится:

- ✓ информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;
- ✓ информация, способная 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, призывающая принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
- ✓ информация, обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;
- ✓ информация, отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
- ✓ информация, оправдывающая противоправное поведение;
- ✓ информация, содержащая нецензурную брань;
- ✓ информация, содержащая информацию порнографического характера.

На сегодняшний день встала очень важная задача необходимости формирования информационной культуры

школьников. Само понятие информационной культуры включает совокупность умений, знаний и навыков поиска, отбора, анализа информации, направленных на удовлетворение потребностей в информации.

Информационную культуру составляют:

– медиаграмотность,
– медиаобразование
– информационная грамотность**.**

Медиаграмотность определяется в международном праве как грамотное использование детьми и их преподавателями инструментов, обеспечивающих доступ к информации, развитие критического анализа содержания информации и формирование коммуникативных навыков, содействие профессиональной подготовке детей и педагогов в целях позитивного и ответственного использования ими информационных и коммуникационных технологий и услуг. Развитие и обеспечение информационной грамотности признаны эффективной мерой противодействия посягательствам на детей с использованием сети Интернет.

Медиаобразование выполняет важную роль в защите детей от негативного воздействия средств массовой коммуникации, способствует осознанному участию детей и подростков в медиасреде и медиакультуре, что является одним из необходимых условий эффективного развития гражданского общества. Медиаобразование выступает здесь как педагогическая система, позволяющая использовать современные методики и технологии.

Разработка и практическая реализация педагогического комплекса формирования и развития информационной культуры - одна из наиболее актуальных задач современной школы. В связи с чем возникла необходимость выработки научного подхода к внедрению в образовательный процесс вопросов обучения грамотного восприятия, анализа и критического отношения к информационному потоку, которому подвергается любой школьник.

Информационная грамотность - это комплекс умений работать с информацией – классифицировать ее по заданным признакам, собирать, фильтровать, преобразовывать из одной

формы в другую, излагать в соответствии с заданными параметрами.

Интернет занимает важную часть жизни человека. Это не только информационный и социальный, но и развлекательный ресурс, что особенно привлекает детей. Сегодня они начинают пользоваться сетью Интернет довольно рано, а в школьные годы уже владеют технологиями лучше многих взрослых. К сожалению, Интернет не так безопасен, как может показаться с первого взгляда. В нем существует огромное количество угроз, которые могут негативно сказаться на ребенке. **К** таким **угрозам** относятся:

– доступная для детей негативная информация;

– мошенники, онлайн-игроки и другие лица, прививающие детям склонность к азартным играм, выманивающие у детей конфиденциальную информацию о родителях и уровне материальной обеспеченности семьи, а также ставящие ребенка в материальную и иную зависимость;

– педофилы, для которых дети становятся объектами развратных действий и преступлений;

– сектанты, навязывающие нетрадиционные, асоциальные отношения и ценности;

– противоправные и социально-опасные действия самого ребенка;

– кибербуллеры-злоумышленники, которые унижают и «травят детей»;

– призыв к суициду и игры со смертью;

– селфхарм (преднамеренное повреждение своего тела по внутренним причинам без суицидальных намерений);

– экстремальные селфи;

– сайты «для взрослых»;

– различные радикальные движения против родителей и семьи, школ и педагогов.

В интерактивном мире дети могут быть так же беззащитны, как и в реальном. Поэтому важно сделать все возможное, чтобы защитить их.

Проблемы безопасности детей в интернете волнуют педагогическое сообщество, поскольку в школе активно используются интернет-ресурсы. Обеспечить безопасность

школьной сети помогут специальные фильтры, закрывающие доступ к опасным сайтам, что является заботой администрации.

Чтобы обеспечить медиабезопасность в ходе образовательного процесса педагоги должны быть к этому готовы, поэтому должна вестись целенаправленная работа с учителями.

Для этого необходимо:

1. Изучить технику безопасности в сети Интернет, чтобы знать виды Интернет-угроз, уметь их распознать и предотвратить.
2. Уметь определять, какими функциями обладают компьютеры, планшеты, а также какое программное обеспечение на них установлено.
3. Учитель обязан рассказать школьнику как можно больше о виртуальном мире, его возможностях и опасностях.
4. Педагог не должен позволять в ходе образовательного процесса учащимся самостоятельно исследовать Интернет-пространство, они могут столкнуться с агрессивным контентом.
5. Педагог должен сам выбирать интересные ресурсы и предлагать их на учебном занятии.
6. Учителю необходимо проверять правильность установки и настройки средств фильтрации контента, спама и антивирусов.

Медиабезопасность в семье

Дети начинают пользоваться Интернетом во все более и более раннем возрасте. Однако у тех, кто еще не достиг десятилетнего возраста, обычно нет навыков критического мышления, столь необходимых для самостоятельного посещения Интернета. Поэтому всякий раз, когда дети выходят в сеть, родителям необходимо быть рядом и следить за тем, чтобы они посещали только те сайты, которые выбрали родители.

Родителям следует выработать вместе с детьми соглашение по использованию Интернета. В нем должны быть описаны права и обязанности для каждого члена семьи, четко сформулированы следующие пункты:

- ✓ Какие сайты могут посещать дети и что им разрешается там делать.
- ✓ Сколько времени дети могут проводить в Интернете.

✓ Что делать, если что-либо вызывает у ваших детей ощущение дискомфорта.

✓ Как защитить личные данные.

✓ Как следить за безопасностью.

✓ Как вести себя при общении.

✓ Как пользоваться службами чатов, группами новостей и мгновенными сообщениями.

Для эффективности такого соглашения крайне важно участие детей в его составлении. Распечатайте соглашение и держите рядом с компьютером для напоминания всем членам семьи, регулярно просматривайте, вносите изменения по мере того, как дети взрослеют.

Взрослым необходимо научить ребенка быть осторожным при знакомстве с новыми людьми в Интернете.

Родителям необходимо знать, с кем контактирует в Интернете ребенок. Для этого необходимо проверять все контакты детей, чтобы убедиться, что они лично знают всех, с кем общаются. Необходимо объяснить, что нельзя разглашать в Интернете информацию личного характера, например, номер телефона, домашний адрес, название/номер школы, а также пересылать интернет-знакомым свои фотографии.

Если ребенок интересуется контактами с людьми намного старше его, следует провести разъяснительную беседу. Не позволяйте вашему ребенку встречаться с онлайн-знакомыми без Вашего разрешения или в отсутствии взрослого человека. Если ребенок желает встретиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу. Интересуйтесь тем, куда и с кем ходит ваш ребенок.

Необходимо также научить ребенка правильному общению в сети Интернет.

Дети часто общаются в сети на форумах, в социальных сетях, в блогах, пишут комментарии. Они высказывают свои точки зрения. Иногда мнения не сходятся, и начинается словесная перепалка, переходящая в состояние хамства, оскорбления, угроз. Необходимо объяснять детям, что в сети Интернет правила хорошего тона ничем не отличаются от правил в повседневной жизни. Нужно объяснить детям, что

нельзя использовать Сеть для хулиганства, распространения угроз.

Но в тоже время и сам ребенок может стать жертвой хулиганства в сети Интернет. Это можно заметить по поведению ребенка. Переживания, замкнутость, отчужденность, плохое настроение, потеря интереса к Интернету, депрессии, жалобы на головную боль – это могут быть симптомы того, что ребенку угрожает какая-либо опасность в Интернете. В этом случае необходимо проверить все контакты и действия ребенка в сети.

Профилактика Кибер-издевательства

Наряду со всеми преимуществами современной беспрецедентной информационной взаимосвязи, приходят и определенные опасности. Мы живем в мире мгновенных коммуникаций и доступа — в Интернете, новости (особенно плохие) распространяются чрезвычайно быстро и повсюду, прежде чем можно что-либо сделать, чтобы контролировать их. Детям и подросткам, эта мгновенная и распространяющаяся доступность, может причинить серьезные проблемы. Дети способны к подстрекательству слухов и угроз, которые могут довести других детей до состоянии полного отчаяния.

Все мы видели в новостях рассказы о детях, которые становились жертвами кибер-издевательства, и слишком часто это доводило их до самоубийства. И вместо того, чтобы быть изолированными инцидентами в нескольких странах, кибер-издевательство, кажется, стало полноправной эпидемией с увеличивающимися случаями по всему миру. На самом деле, некоторые исследования показали, что более сорока процентов всех подростков испытали некоторую форму кибер-издевательства, и каждый четвертый подросток сообщил, что почувствовал это на себе не раз.

Это тревожная статистика, учитывая тот факт, что кибер-издевательство действительно может убить. Подростки - эмоциональные существа, и часто могут переживать трудные времена, не видя выхода из отрицательно-влияющей социальной дилеммы. Многие подростки боятся сообщать о случаях издевательства своим родителям или школьной администрации, потому что опасаются дальнейших взаимных обвинений от

хулиганов, которые их мучают. Эти ситуации могут быстро перерасти в чувство полного отчаяния, в которых подросток чувствует себя загнанным в ловушку и не видит выхода из нее.

Просто подобного рода чувства, заставили многих подростков в различных городах по всему миру, положить конец своей жизни. И много раз, родители и учителя не имели понятия, о том, что что-то было не так, пока не стало слишком поздно. Эти инциденты происходят во всех слоях общества – благосостояние или бедность, кажется оказывает незначительное влияние на то, кому навредить. В наше время почти у всех детей – богатых или бедных – есть смартфоны или планшеты, и социальная сеть – один из главных инструментов, используемых для поддержания отношений и обмена информацией.

Старая пословица "плохие новости распространяются быстро", особенно применима в кибер-эпоху. Плохие новости не только распространяются быстро, но также могут распространяться далеко и широко, в очень короткое время. Одна из опасностей кибер-издевательства заключается в том, что слухи, смущающая информация или уличающее видео и фотографии, могут быть распространены чрезвычайно быстро среди очень широкой аудитории.

Этот "мгновенный" аспект интернета является частью того, что может сделать кибер-издевательство таким угрожающим. Больше не существует издевательства с руганью и распространением слухов среди нескольких сверстников - кибер-издевательство может включать сотни и даже тысячи свидетелей или участников. Иногда нам, кто вырос в эпоху до того, как социальные сети в интернете стали настолько популярными, трудно понять потенциал и объем того, что может случиться в Интернете в течение нескольких часов или даже минут.

Методы кибер-издевательства

Кибер-издевательство может принимать различные формы. Часто это может быть просто распространение слухов в Facebook или других соц. сетях, но существует несколько очень сложных и изощренных тактик, которые используются в наше время. Родители должны быть осведомлены о том, что

технически подкованные подростки, желающие издеваться на другими имеют широкий выбор средств в их распоряжении. Вот лишь некоторые из страшных методов, которые используют современные кибер-хулиганы для издевательств и пытки своих жертв:

Ratting - включает в себя установку вредоносного приложения на чей-либо компьютер, что позволяет хакеру наблюдать за жертвой через веб-камеру компьютера. Изображения или видео, сделанные тайком затем могут быть использованы, чтобы смутить или шантажировать невольного подростка. Это может показаться продвинутым методом взлома для технически не подкованных родителей, но многие дети обладают навыками, для выполнения такого рода нападений на частную жизнь.

Фальшивый профиль - относительно легко создать фальшивый профиль в социальных сетях. Все, что вам нужно это имя и фотография для создания профиля, в таких социальных сетях, как Facebook и Twitter. Хулиган выдавая себя за другого человека может создать фальшивый профиль, который был создан, чтобы высмеивать или смущать его, дурача других, которые думают, что профиль на самом деле был создан жертвой.

Digital Pile-Ons - это просто группа людей, которая объединяется в социальной сети, типа Facebook для того, чтобы писать подлые комментарии о человеке. Один человек начинает поливать грязью кого-то, а другие присоединяются, чтоб нагнетать обстановку. Это одна из наиболее распространенных форм кибер-издевательства.

Что могут сделать родители, чтобы защитить своих детей от кибер-издевательства?

Приведенные выше тактики, это всего лишь несколько примеров использования интернета детьми для того, чтобы сделать жизнь другого ребенка несчастной. Родители должны сначала осознать, насколько широко распространенным и мощным стало кибер-издевательство. Это не изолированное явление, это повседневная реальность для большинства подростков. Даже если они не являются подстрекателями или

жертвой, вполне вероятно, что они знают тех, кто участвует в этом, независимо от того страдают ли сами, выступают в роли преступников, или и то и другое.

Родители и дети должны быть осведомленны об опасностях кибер-издевательства и владеть средствами борьбы с ним. Многие школы сейчас предлагают семинары по данному вопросу, и родители должны приложить все усилия, чтобы посещать их или по крайней мере, самостоятельно изучить вопрос о том, как бороться и предотвратить кибер-издевательство над собственными детьми.

Обсудите проблему со своими детьми. Важно, чтобы ваши дети знали, что вы осведомлены о потенциале кибер-издевательства, и что вы рядом, чтобы поддержать их от любых нападений подобного рода. Пусть ваши дети знают, что они не будут наказаны за то, что сообщат вам информацию, касающуюся таких атак, даже если она будет компрометирующей и будет содержать интимные подробности жизни вашего ребенка. Дайте им понять, что вы рядом, чтоб поддержать их, независимо от того, насколько ужасной может показаться ситуация.

Управляйте интернет активностью вашего ребенка. Убедитесь, что вы контролируете интернет активность вашего ребенка, и не забудьте внимательно следить за их взаимодействиями. Вы должны быть администратором их смартфонов, планшетов, ноутбуков и настольных ПК - убедитесь, что вы знаете пароли к сайтам социальных сетей.

Вы имеете полное право и обязаны управлять и контролировать интернет поведение Вашего ребенка. Ребенок должен заслужить доверие и автономию — вы не должны совать нос в любую его деятельность в Интернете, но важно иметь четкое представление об общем поведении вашего ребенка онлайн, и получить ясную картину о том, с кем он общается.

Используйте мобильную программу для мониторинга, чтоб защитить своего ребенка.

Одним из наиболее эффективных способов контроля интернет активности вашего ребенка, является установка программного обеспечения для мониторинга смартфонов — так называемое "Приложение трекер для телефонов". Эти мобильные

приложения позволяют просматривать все, что происходит на целевом телефоне или планшете, в том числе местоположение GPS. Это очень полезные инструменты для слежения за тем, какой информацией обменивается ваш подросток, с кем общается и где проводит свое время.

Эти приложения просты в установке и использовании, и абсолютно необнаружимы пользователем телефона. Так что, это зависит от родителей, сообщать или нет ребенку о том, что он находится под наблюдением. Эти мобильные приложения мониторинга становятся очень популярными среди родителей, которые обеспокоены кибер-издевательством, а также многими другими потенциальными угрозами, которым подвергаются дети в интернете.

Взрослым следует предпринять меры безопасности, если ребенок использует такие хеш-теги: #f53 #f57 #f58 #d28 #морекитов #тихийдом #хочувигру #млечныйпуть #хочувигру #ждуинструкцию или состоит в группах, содержащих в названии следующее: «Киты плывут вверх», «Разбуди меня в 4.20», «f57», «f58», «Тихийдом», «Рина», «Няпока», «Море китов», «50 дней до моего...», «домкитов», «млечныйпуть», «150звёзд», «ff33», «d28», «хочувигру», или постоянно рисует китов, бабочек, единорогов не только на бумаге, но и на своем теле.

Для защиты детей от опасностей в Интернете необходима активная позиция родителей. «Родительский контроль» — не только определение из психологии или причина детской жалобы. В информационной среде данный термин применим к группе программ, которые ограничивают доступ к использованию вредных, опасных или негативно влияющих на ребенка интернет ресурсов.

Программы, которые рекомендуется использовать с этой целью:

1. ChildWebGuardian Pro.
2. Hidetools Parental Control.
3. KinderGate Parental Control.
4. Kids PC Time Administrator.

Программа «Родительский контроль» позволяет:

– сформировать списки контактов, переписка с которыми будет разрешена или запрещена;

– задать ключевые слова, наличие которых будет проверяться в сообщениях;

– указать личную информацию, пересылка которой будет запрещена.

Если переписка с контактом запрещена, то все сообщения, адресованные этому контакту или полученные от него, будут блокироваться. Информация о заблокированных сообщениях, а также о наличии ключевых слов в сообщениях выводится в отчет. Для каждой учетной записи пользователя компьютера можно посмотреть краткую статистику переписки через социальные сети, а также подробный отчет о событиях.

Медиабезопасность детей в сети Интернет должна обеспечиваться совместными усилиями школы и родителей. В школе может быть разработана программа по медиабезопасности, которая включает в себя уроки и внеклассные мероприятия по медиабезопасности, неделю медиавбезопасности, тематические модули по медиабезопасности в рамках предметов технология или информатика, мероприятия по медиабезопасности для родителей.

В настоящее время интенсивно обсуждается и исследуется феномен «наркозависимости от Интернета», или **Интернет-аддикции**.

В самом общем виде Интернет-зависимость (Internet addiction) определяется как «нехимическая зависимость от пользования Интернетом». Поведенчески Интернет-зависимость проявляется в том, что люди настолько предпочитают жизнь в Интернете, что фактически начинают отказываться от своей «реальной» жизни, проводя до 18 часов в день в виртуальной реальности. Другое определение Интернет-зависимости - это «навязчивое желание войти в Интернет, находясь off-line, и неспособность выйти из Интернет, будучи on-line».

В 1998-1999 гг. опубликованы первые монографии но данной проблеме (К. Янг, Д. Гринфилд. К. Сурратт). Кимберли Янг приводит 4 симптома Интернет-аддикции:

- навязчивое желание проверить e-mail;
- постоянное ожидание следующего выхода в Интернете;

- жалобы окружающих на то, что человек проводит слишком много времени в Интернет;
- жалобы окружающих на то, что человек тратит слишком много денег на Интернет.

Часто Интернет-аддикция понимается гораздо шире. Сюда относят зависимость от компьютера, т.е. пристрастие к работе с компьютером (играм, программированию или другим видам деятельности); «информационную перегрузку», т.е. компульсивную навигацию по WWW, поиск в удаленных базах данных; компульсивное применение Интернета, т.е. патологическую привязанность к азартным играм, онлайновым аукционам или электронным покупкам в Интернете; зависимость от «кибер-отношений», т.е. от социальных применений Интернета - общения в чатах, групповых играх и телеконференциях, что может в итоге привести к замене имеющихся в реальной жизни семьи и друзей виртуальными.

Что нас ждет в недалеком будущем?

– Стирание границ между онлайн и оффлайн.

– Повышение ответственности за свои действия в сети.

– Видоизменение или полный отказ от самого понятия анонимности в сети.

– Публичность как необходимое условие существования.

10 худших паролей из топ-100 2017 года

1. 123456
2. password
3. 12345678
4. Qwerty
5. 12345
6. 123456789
7. letmain
8. 1234567
9. football
10. iloveyou

Способы повышения безопасности

1. Соблюдайте законы.
2. Старайтесь избегать постоянных логинов и паролей при регистрации на различных сайтах.

3. Придерживайтесь географической удаленности при регистрации – если регистрируетесь на Facebook, то предпочтительнее использовать Российскую электронную почту.
4. Правильная настройка средств общения.
5. Понимание того, что поведение в сети хоть и специфично, но всё-таки мало отличается от поведения в жизни.

Информация предоставлена Образовательным порталом для педагогов, школьников и родителей «Знанио»
https://spycellphone.mobi/ru/профилактика-кибер-издевательства
https://psyera.ru/internet-addikciya-366.htm