

Красноярский краевой институт повышения
квалификации и профессиональной переподготовки
работников образования
Центр воспитания и гражданского образования



Методические материалы для проведения в организациях дошкольного, начального общего, основного общего, среднего (полного) общего образования, среднего профессионального образования, дополнительного образования детей, в организациях для детей-сирот и детей, оставшихся без попечения родителей, мероприятий по основам информационной безопасности детей («основы медиабезопасности»)

Материалы составлены по заказу министерства образования и науки Красноярского края в соответствии с поручением Первого заместителя Губернатора края – председателя Правительства края В.П.Томенко, данным по обращению Уполномоченного при Президенте России по правам ребенка П.А.Астахова к Губернатору Красноярского края Л.В.Кузнецову о поддержке Всероссийской информационной компании против насилия и жестокости в СМИ и других средствах массовой коммуникации (2013 – 2014гг.)

Составитель: Пригодич Елена Григорьевна, руководитель Центра воспитания и гражданского образования КК ИПКиППРО

Красноярск 2013

Содержание

1. Введение	с. 3 – 4
2. Рекомендации по проведению уроков и родительских собраний по медиабезопасности школьников, разработанные отделом по обеспечению деятельности Уполномоченного при Президенте Российской Федерации по правам ребенка	с.5 - 45
2.1. Понятия. Цели и задачи проведения уроков и родительских собраний по медиабезопасности с.5-7	
2.2. Нормативная правовая база защиты детей от опасной информации с.7-14	
2.3. Актуальность обеспечения медиабезопасности детей и подростков с.14 - 20	
2.4. Виды он-лайн угроз, представляющих опасность для жизни и развития ребенка с.20 - 39	
2.5. Государственные органы и общественные организации, занимающиеся проблемами защиты детей в киберпространстве с.39 - 44	
2.6. Полезные ссылки с.45	
3. Ссылки на видео-выступления П.А.Астахова по медиабезопасности детей	с. 45
4. Рекомендации для проведения занятий с детьми и родительских собраний по медиабезопасности с учетом возрастных особенностей	с.46-57
4.1. В учреждениях дошкольного образования с.46-47	
4.2. Для учащихся 2 – 4 классов – марафон «Медиабезопасность» с.48 - 50	
4.3. Занятия с учащимися 5 – 7 классов в формате классных часов с.50 - 52	
4.4. С учащимися 8 – 9 классов - круглый стол по обсуждению советов корпорации Майкрософт с.52 - 56	
4.5. Старшеклассники – организаторы мероприятий по медиабезопасности в начальной и основной школе с.57	
5. Советы родителям «Как помочь вашим детям более безопасно пользоваться сайтами социальных сетей?»	с.57 - 60
6. Обучение детей основам безопасности при работе с Интернетом	с.60-63

Методические рекомендации «Основы медиабезопасности»

7. Советы по медиабезопасности от сотовой компании «Мегафон».....с.63-65

1. Введение

С 1 сентября 2012 года вступил в силу Федеральный закон № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию". Уполномоченный при Президенте Российской Федерации по правам ребенка П.А.Астахов отметил, что для современной России этот закон имеет огромное политическое, общественное и духовно-нравственное значение: "Он создаёт отсутствовавшую до сих пор и остро необходимую обществу правовую основу для защиты семьи и несовершеннолетних от деструктивного влияния информационной среды, охраны психического и нравственного здоровья детей... Зачастую дети принимают все, что видят по телевизору и в Интернете, за чистую монету. В силу возраста, отсутствия жизненного опыта и знаний в области медиаграмотности они не всегда умеют распознать манипулятивные техники, используемые при подаче рекламной и иной информации, не анализируют степень достоверности информации и подлинность ее источников. Мы же хотим, чтобы ребята стали полноценными гражданами своей страны – теми, кто может анализировать и критически относиться к информационной продукции. Они должны знать, какие опасности подстерегают их в сети и как их избежать".

1 октября 2012 года на VI Съезде Уполномоченных по правам ребёнка в субъектах Российской Федерации Павел Астахов заявил: "С 1 января 2013 года мы запускаем Общероссийскую кампанию против насилия и жестокости в СМИ, включающую комплекс мер информационного, обучающего и организационного характера, в том числе направленных на информирование родителей, педагогов, воспитателей, профессионального журналистского сообщества и интернет-сообщества о вреде, причиняемом современными средствами коммуникации психическому развитию". Уполномоченный считает необходимым совершенствовать законодательство в сфере защиты детей от информации, причиняющей вред их здоровью и развитию (в том числе в части распространения его действия на участие детей в публичных зрелищных мероприятиях - телешоу, приемах и пр.). Перспективным является развитие системы обучения

несовершеннолетних, их родителей, педагогов и воспитателей основам медиабезопасности.

В рамках Плана Всероссийской информационной кампании против насилия и жестокости в СМИ и других средствах массовой коммуникации во всех регионах России в сентябре – декабре 2013г. в организациях дошкольного, начального общего, основного общего, среднего (полного) общего образования, среднего профессионального образования, дополнительного образования детей, в организациях для детей-сирот и детей, оставшихся без попечения родителей, организациях, осуществляющие лечение, оздоровление и (или) отдых детей, организациях, осуществляющих социальное обслуживание детей и других организациях, осуществляющих обучение несовершеннолетних, организуется: проведение занятий для детей, их родителей и воспитателей по основам информационной безопасности детей («основы медиабезопасности»); обеспечение современными программно-техническими средствами (сетевыми экранами (фильтрами), исключающими доступ обучающихся и воспитанников к ресурсам сети Интернет, несовместимым с задачами воспитания; проведение специальных мероприятий по вопросам информационной безопасности несовершеннолетних: конкурса детского рассказа и рисунка «Телевизор - мой друг, телевизор – мой враг», конкурса «Открытого письма телевещателям», конкурса детских СМИ; проведение общешкольных тематических родительских собраний «Как защитить ребенка от негативного контента в СМИ и Интернете».

В настоящих методических материалах представлены рекомендации по проведению родительских собраний и уроков по медиабезопасности школьников, разработанные отделом по обеспечению деятельности Уполномоченного при Президенте Российской Федерации по правам ребенка, а также рекомендации по проведению занятий по медиабезопасности с учетом возрастных особенностей учащихся, разработанные методистами Центра воспитания и гражданского образования Красноярского краевого ИПКи ППРО.

2. Рекомендации по проведению уроков и родительских собраний по медиабезопасности школьников

О.В. Пристанская, начальник отдела по обеспечению деятельности Уполномоченного при Президенте Российской Федерации по правам ребенка

2.1. Понятия. Цели и задачи проведения уроков и родительских собраний по медиабезопасности.

Идея проведения акции по проведению уроков медиабезопасности принадлежит Уполномоченному при Президенте Российской Федерации по правам ребенка Павлу Астахову: «Зачастую дети принимают все, что видят по телевизору и в Интернете, за чистую монету. В силу возраста, отсутствия жизненного опыта и знаний в области медиаграмотности они не всегда умеют распознать манипулятивные техники, используемые при подаче рекламной и иной информации, не анализируют степень достоверности информации и подлинность ее источников. Мы же хотим, чтобы ребята стали полноценными гражданами своей страны – теми, кто может анализировать и критически относиться к информационной продукции. Они должны знать, какие опасности подстерегают их в сети и как их избежать». Данная инициатива была поддержана Президентом Российской Федерации Дмитрием Медведевым 30 мая 2011 года на заседании Президиума Государственного совета Российской Федерации и Комиссии по реализации приоритетных национальных проектов и демографической политике, посвящённом вопросам охраны здоровья детей и подростков.

Медиаграмотность определяется в международном праве как грамотное использование детьми и их преподавателями инструментов, обеспечивающих доступ к информации, развитие критического анализа содержания информации и привития коммуникативных навыков, содействие профессиональной подготовке детей и их 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 (Рекомендация Rec 2006) 12 Комитета министров государствам-членам Совета Европы по расширению возможностей детей в новой информационно-коммуникационной среде от 27.09.2006

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. Обеспечение государством информационной безопасности детей, защита их физического,

умственного и нравственного развития во всех аудиовизуальных медиа-услугах и электронных СМИ – требование международного права (Рекомендации Европейского Парламента и Совета ЕС от 20.12.2006 о защите несовершеннолетних и человеческого достоинства в Интернете, Решение Европейского парламента и Совета № 276/1999/ЕС о принятии долгосрочной плана действий Сообщества по содействию безопасному использованию Интернета посредством борьбы с незаконным и вредоносного содержимого в рамках глобальных сетей).

Согласно российскому законодательству *информационная безопасность детей* – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию (Федеральный закон от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию"). Такую защищенность ребенку должны обеспечить, прежде всего, семья и школа. Это задача не только семейного, но и школьного воспитания. Проведение уроков медиабезопасности планируется в образовательных учреждениях на постоянной основе, начиная с первого класса, в рамках школьной программы (в том числе уроков ОБЖ).

Цель проведения уроков медиабезопасности – обеспечение информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

Задачи уроков медиабезопасности:

1) информирование учащихся о видах информации, способной причинить вред здоровью и развитию несовершеннолетних, запрещенной или ограниченной для распространения на территории Российской Федерации, а также о негативных последствиях распространения такой информации;

2) информирование учащихся о способах незаконного распространения такой информации в информационно-телекоммуникационных сетях, в частности, в сетях Интернет и мобильной (сотовой) связи (в том числе путем рассылки SMS-сообщений незаконного содержания);

3) ознакомление учащихся с международными принципами и нормами, с нормативными правовыми актами РФ, регулирующими вопросы информационной безопасности несовершеннолетних;

4) обучение детей и подростков правилам ответственного и безопасного пользования услугами Интернет и мобильной (сотовой) связи, другими электронными средствами связи и коммуникации, в том числе способам защиты от противоправных и иных общественно опасных посягательств в информационно-телекоммуникационных сетях,

в частности, от таких способов разрушительного воздействия на психику детей, как кибербуллинг (жестокое обращение с детьми в виртуальной среде) и буллицид (доведение до самоубийства путем психологического насилия);

5) профилактика формирования у учащихся интернет-зависимости и игровой зависимости (игромании, гэмблеринга);

6) предупреждение совершения учащимися правонарушений с использованием информационно-телекоммуникационных технологий.

Ожидаемые результаты.

В ходе уроков медиабезопасности дети должны научиться сделать более безопасным и полезным свое общение в Интернете и иных информационно-телекоммуникационных сетях, а именно:

- критически относиться к сообщениям и иной информации, распространяемой в сетях Интернет, мобильной (сотовой) связи, посредством иных электронных средств массовой коммуникации;
- отличать достоверные сведения от недостоверных, вредную для них информацию от безопасной;
- избегать навязывания им информации, способной причинить вред их здоровью, нравственному и психическому развитию, чести, достоинству и репутации;
- распознавать признаки злоупотребления их неопытностью и доверчивостью, попытки вовлечения их в противоправную и иную антиобщественную деятельность;
- распознавать манипулятивные техники, используемые при подаче рекламной и иной информации;
- критически относиться к информационной продукции, распространяемой в информационно-телекоммуникационных сетях;
- анализировать степень достоверности информации и подлинность ее источников;
- применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях.

2.2. Нормативная правовая база защиты детей от информации, причиняющей вред их здоровью, репутации, нравственному, духовному и социальному развитию.

Защита детей от информации, причиняющей вред их здоровью, репутации и развитию, регулируется:

– нормами международного права — ст. 13, 17, 34 Конвенции ООН о правах ребенка 1989 г., Европейской декларацией о свободе обмена информацией в Интернете 2003 г., Европейской конвенцией о совместном кинопроизводстве 1992 г., Европейской конвенцией о трансграничном телевидении 1989 г. (Россия не участвует), Европейской конвенцией о правонарушениях в сфере электронной информации 2001 г. (Россия не участвует - Распоряжение Президента Российской Федерации «О признании утратившим силу распоряжения Президента Российской Федерации от 15.11.2005 № 557-рп “О подписании Конвенции о киберпреступности”» от 22.03.2008 № 144-рп); Европейской рамочной конвенцией о безопасном использовании мобильных телефонов маленькими детьми и подростками (06.02.2007); Рекомендациями Комитета Министров государств — членов Совета Европы: № R (89) 7 — относительно принципов распространения видеозаписей, содержащих насилие, жестокость или имеющих порнографическое содержание (22.04.1989), № R (97) 19 — о демонстрации насилия в электронных средствах массовой информации (30.10.1997), Рекомендация Rec (2001) 8 – в сфере регулирования в отношении кибер-контента (саморегулирования и защиты пользователей от незаконного или вредного содержания новых коммуникаций и информационных услуг), № Rec (2003) 9 – о мерах поддержки демократического и социального распространения цифрового вещания (28.05.2003), Рекомендации Rec (2006) 12 по расширению возможностей детей в новой информационно-коммуникационной среде (27.09.2006), CM/Rec (2007) 11 о поощрении свободы выражения мнений и информации в новой информационной и коммуникационной среде, CM/Rec (2008) 6 о мерах по развитию уважения к свободе слова и информации в связи с Интернет-фильтрами; Рекомендациями Европейского парламента и Совета ЕС о защите несовершеннолетних и человеческого достоинства и права на ответ в отношении конкурентоспособности индустрии европейских аудиовизуальных и информационных он-лайн услуг (20.12.2006); Модельным законом МПА СНГ «О противодействии торговле людьми», принятым на тридцатом пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ (03.04.2008); Рекомендациями по унификации и гармонизации законодательства государств – участников СНГ в сфере борьбы с торговлей людьми (03.04.2008); Модельным законом МПА СНГ «О защите детей от информации, причиняющей вред их здоровью и развитию» (03.12.2009); Рекомендациями по унификации и гармонизации законодательства государств – участников СНГ в сфере защиты детей от информации, причиняющей вред их здоровью и развитию (28.10.2010);

- **федеральным законодательством** — ст. 14, 14.1 Федерального закона от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации», ст. 31 Основ законодательства Российской Федерации о культуре от 09.10.1992 № 3612-1, ст. 4, 37 Закона Российской Федерации от 27.12.1991 «О средствах массовой информации» № 2124-1, ст. 46 Федерального закона от 08.01.1998 № 3-ФЗ «О наркотических средствах и психотропных веществах», Федеральным законом от 13.03.2006 № 38-ФЗ «О рекламе», Федеральным законом от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" (вступает в действие 01.09.2012), Федеральный закон от 21.07.2011 № 252-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О защите детей от информации, причиняющей вред их здоровью и развитию" (вступает в действие 01.09.2012), а также Стратегией национальной безопасности Российской Федерации до 2020 года, утвержденной Указом Президента Российской Федерации от 12.05.2009 № 537, и Доктриной информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации 09.09.2000 № ПР-1895, в которых закреплены общие принципы обеспечения информационной безопасности граждан и государства;
- **нормативными правовыми актами субъектов Российской Федерации;**
- **Приказом Генерального прокурора Российской Федерации** от 26.11.2007 № 188 «Об организации прокурорского надзора за исполнением законов о несовершеннолетних и молодежи» (п. 3.2) – предусмотрено проведение систематических проверок соблюдения законодательства о защите детей от информации, наносящей вред их здоровью, репутации, нравственному и духовному развитию, в деятельности средств массовой информации, органов и учреждений образования и культуры. Прокуроры должны привлекать к установленной ответственности юридических и физических лиц, виновных в распространении указанной информации или пропагандирующих насилие и жестокость, порнографию, наркоманию, антиобщественное поведение, в том числе употребление алкоголя, наркотиков, табачных изделий, а также пресекать в пределах предоставленных законом полномочий использование средств массовой информации и информационно-телекоммуникационных сетей, в том числе сети Интернет, для сексуальной эксплуатации и совершения иных преступлений против несовершеннолетних.

Для сведения. *Федеральный закон № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»* устанавливает правила медиабезопасности детей при обороте 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 подвижной радиотелефонной связи.

Он содержит ряд новационных норм, предусматривающих создание организационно-правовых механизмов защиты детей от распространения в сети Интернет вредной для них информации (возрастную классификацию информационной продукции, ее маркировку, применение сертифицированных технических и программно-аппаратных средств). Устанавливаются требования к распространению среди детей информации, в том числе требования к осуществлению классификации информационной продукции, ее экспертизы, государственного надзора и контроля за соблюдением законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию.

Согласно новому закону доступ детей к информации, распространяемой посредством информационно-телекоммуникационных сетей, может предоставляться операторами связи в Интернет-кафе, образовательных и других учреждениях, в пунктах коллективного доступа только при условии применения ими технических, программно-аппаратных средств защиты детей.

В информационной продукции для детей, в том числе размещаемой в информационно-телекоммуникационных сетях (включая сеть Интернет) и сетях подвижной радиотелефонной связи, не допускается размещать объявления о привлечении детей к участию в создании информационной продукции, причиняющей вред их здоровью и (или) развитию.

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: 1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству; 2) 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, 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 или животным, за исключением случаев, предусмотренных настоящим Федеральным законом; 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, ограниченной для распространения среди детей определенных возрастных категорий, относится информация: 1) 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 том числе представляемая в виде изображения или описания 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 бране.

Согласно действующей до вступления в силу указанного Федерального закона от 21.07.2011 № 252-ФЗ редакции *статьи 14 Федерального закона «Об основных гарантиях прав ребенка в Российской Федерации»* органы государственной власти Российской Федерации принимают меры по защите ребенка от информации, пропаганды и агитации, наносящих вред его здоровью, нравственному и духовному развитию, в том числе от национальной, классовой, социальной нетерпимости, от рекламы алкогольной продукции и табачных изделий, от пропаганды социального, расового, национального и религиозного неравенства, а также от распространения печатной продукции, аудио- и видеопродукции, пропагандирующей насилие и жестокость, порнографию, наркоманию, токсикоманию, антиобщественное поведение.

В целях обеспечения здоровья, физической, интеллектуальной, нравственной, психической безопасности детей федеральным законом, законами субъектов Российской Федерации устанавливаются нормативы распространения печатной продукции, аудио- и видеопродукции, иной

продукции, не рекомендуемой ребенку для пользования в соответствии с пунктом 1 настоящей статьи до достижения им возраста 18 лет.

В соответствии со *статьей 14.1. Федерального закона «Об основных гарантиях прав ребенка в Российской Федерации»* (введена Федеральным законом от 28.04.2009 № 71-ФЗ) в целях содействия физическому, интеллектуальному, психическому, духовному и нравственному развитию детей и формированию у них навыков здорового образа жизни органы государственной власти Российской Федерации, органы государственной власти субъектов Российской Федерации, органы местного самоуправления в соответствии с их компетенцией создают благоприятные условия для осуществления деятельности организаций, образующих социальную инфраструктуру для детей (включая места для их доступа к сети "Интернет").

Законами субъектов Российской Федерации в целях предупреждения причинения вреда здоровью детей, их физическому, интеллектуальному, психическому, духовному и нравственному развитию могут устанавливаться, в частности, меры по недопущению нахождения детей (лиц, не достигших возраста 18 лет) в ночное время в общественных местах, в том числе на объектах (на территориях, в помещениях) юридических лиц или граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, которые предназначены для обеспечения доступа к сети "Интернет" и в иных общественных местах без сопровождения родителей (лиц, их заменяющих) или лиц, осуществляющих мероприятия с участием детей.

За несоблюдение установленных требований к обеспечению родителями (лицами, их заменяющими), лицами, осуществляющими мероприятия с участием детей, а также юридическими лицами или гражданами, осуществляющими предпринимательскую деятельность без образования юридического лица, мер по содействию физическому, интеллектуальному, психическому, духовному и нравственному развитию детей и предупреждению причинения им вреда законами субъектов Российской Федерации может устанавливаться административная ответственность.

В целях защиты несовершеннолетних от злоупотреблений их доверием и недостатком опыта Федеральным законом от 13.03.2006 № 38-ФЗ «О рекламе» установлен комплекс ограничений при распространении рекламной продукции.

В рекламе (в том числе распространяемой в информационно-телекоммуникационных сетях) не допускаются (ст. 6): 1) дискредитация родителей и воспитателей, подрыв доверия к ним у

несовершеннолетних; 2) побуждение несовершеннолетних к тому, чтобы они убедили родителей или других лиц приобрести рекламируемый товар; 3) создание у несовершеннолетних искаженного представления о доступности товара для семьи с любым уровнем достатка; 4) создание у несовершеннолетних впечатления о том, что обладание рекламируемым товаром ставит их в предпочтительное положение перед их сверстниками; 5) формирование комплекса неполноценности у несовершеннолетних, не обладающих рекламируемым товаром; 6) показ несовершеннолетних в опасных ситуациях; 7) преуменьшение уровня необходимых для использования рекламируемого товара навыков у несовершеннолетних той возрастной группы, для которой этот товар предназначен; 8) формирование у несовершеннолетних комплекса неполноценности, связанного с их внешней непривлекательностью.

Законом запрещено также распространение ненадлежащей рекламы, в том числе: побуждающей к совершению противоправных действий (п. 1 ч. 4 ст. 5 Закона о рекламе); призывающей к насилию и жестокости (п. 2 ч. 4 ст. 5 Закона о рекламе); содержащей демонстрацию процессов курения и потребления алкогольной продукции, а также пива и напитков, изготавливаемых на его основе (п. 5 ст. 5 Закона о рекламе); использующей бранные слова, непристойные и оскорбительные образы, сравнения и выражения (ч. 6 ст. 5 Закона о рекламе).

Действуют ограничения для рекламы, размещаемой в детских и образовательных телепередачах, радиопрограммах и радиопередачах (ч. 7 ст. 14, ч. 6 ст. 15 Закона о рекламе). Установлены ограничения для рекламы отдельных видов продукции, представляющей опасность для здоровья и развития детей: алкогольной продукции (ст. 21), пива и напитков, изготавливаемых на его основе (ст. 22), табака, табачных изделий и курительных принадлежностей (ст. 23), лекарственных средств, медицинской техники, изделий медицинского назначения и медицинских услуг (ст. 24), основанных на риске игр, пари (ст. 27). Такая реклама не должна обращаться к несовершеннолетним и использовать их образы, не может размещаться в предназначенных для несовершеннолетних печатных изданиях, аудио- и видеопродукции.

В настоящее время информационная безопасность детей при просмотре аудиовизуальных произведений регулируется также комплексом установленных законодательством РФ требований к содержанию аудиовизуальной информационной продукции, предназначеннной для распространения среди разных возрастных групп несовершеннолетних.

В целях упорядочения публичной демонстрации и распространения аудиовизуальных произведений на любых видах

носителей, защиты детей и подростков от аудиовизуальной продукции, которая может нанести вред их здоровью, эмоциальному и интеллектуальному развитию, введена возрастная классификация аудиовизуальных произведений, соответствующая психовозрастным особенностям восприятия зрительской аудиторией: фильм разрешен для показа в любой зрительской аудитории; детям до 12 лет просмотр фильма разрешен в сопровождении родителей; фильм разрешен для показа зрителям, достигшим 14 лет; фильм разрешен для показа зрителям, достигшим 16 лет; фильм разрешен для показа зрителям, достигшим 18 лет (Приказ Роскультуры от 15.03.2005 № 112 (ред. от 01.07.2005) "Об утверждении Руководства по возрастной классификации аудиовизуальных произведений, положения и состава экспертного совета по возрастной классификации аудиовизуальных произведений").

Для исключения доступа учащихся образовательных учреждений к ресурсам сети Интернет, содержащим информацию, несовместимую с задачами образования и воспитания, за счет средств федерального бюджета в федеральных государственных образовательных учреждениях, государственных образовательных учреждений субъектов РФ и муниципальных образовательных учреждений, реализующих общеобразовательные программы начального общего, основного общего и среднего (полного) общего образования, к сети Интернет, предусмотрены внедрение и актуализация системы исключения доступа к интернет-ресурсам, несовместимым с задачами образования и воспитания учащихся, внедрение в этих целях средств контентной фильтрации и иных аппаратно-программных и технико-технологических устройств (Распоряжение 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").

2.3. Актуальность обеспечения медиабезопасности детей и подростков

Проблема обеспечения информационной безопасности детей в информационно-телекоммуникационных сетях становится все более актуальной в связи с существенным возрастанием численности несовершеннолетних пользователей.

За последние годы в результате значительного повышения обеспеченности компьютерами россиян и подключения в рамках национального проекта практически всех школ к Интернету

пользовательская активность российских школьников резко возросла. Данные исследований Фонда Развития Интернет свидетельствуют о высокой степени контакта детей и подростков с негативным контентом и другими рисками интернет-среды(<http://new.soedin.ru/index.php?action=secur&id=830>).

По данным Центра Безопасного Интернета в России 10 миллионов детей в возрасте до 14 лет активно пользуется Интернетом, что составляет 18% интернет-аудитории нашей страны.

Рынок сотовой связи развивается столь же стремительно. В мире мобильными телефонами пользуются 1.600.000.000 молодых юношей и девушек (<http://lolnet.ru/1156-mobilnyy-telefon-i-lyudi.html>).

В России уровень проникновения сотовой связи составил 110% (160 миллионов пользователей). Уже в 2003 году количество мобильных телефонов в России достигло 31,5 млн. и превысило число стационарных аппаратов (Чеберко И. [Телекоммуникации](#). — Коммерсантъ-Власть, № 24 (577), 21 июня 2004 года). В конце февраля 2010 года абонентская база сотовых операторов насчитывала 210,05 млн. пользователей ([Число пользователей сотовой связи в России выросло на 2 миллиона за месяц](#). — Lenta.ru, 23 марта 2010 года).

Как свидетельствуют данные опросов, в Европе мобильные телефоны имеют около 90% детей в возрасте от 12 до 19 лет и около половины - в возрасте 9-12 лет, в некоторых странах вообще принято дарить детям «мобильники» по достижении ими восьми лет. Помимо звонков и коротких сообщений телефоны используются для выхода в интернет, загрузки изображений, музыки, видео, игр.

Пользователи, как правило, считают свой мобильный телефон более личным и защищенным устройством, чем компьютер и не предполагают, что кто-то другой может увидеть просматриваемые ими страницы или ссылки. Сегодня многие сотовые операторы предлагают им взрослый контент помимо того, который абоненты могут получить с WAP-порталов, т.е. Интернет сайтов, созданных специально для мобильной телефонии.

При этом несовершеннолетние меньше, чем взрослые, подготовлены к проблемам, с которыми могут столкнуться в сети, и нередко остаются беззащитными перед ними. Именно дети и подростки сегодня менее всего защищены от потока негативной информации в Сети.

Значительная часть детской аудитории путешествует в сети самостоятельно еще до окончания младших классов. По результатам социологических исследований 88% четырёхлетних детей выходят в

сеть вместе с родителями. В 8-9-летнем возрасте дети всё чаще выходят в сеть самостоятельно. К 14 годам совместное, семейное пользование сетью сохраняется лишь для 7% подростков. Особенно пугает то, что больше половины пользователей сети в возрасте до 14 лет просматривают сайты с нежелательным содержимым. 39% детей посещают порносайты, 19% наблюдают сцены насилия, 16% увлекаются азартными играми. Наркотическими веществами и алкоголем интересуются 14% детей, а экстремистские и националистические ресурсы посещают 11% несовершеннолетних пользователей (http://www.detivrunete.ru/nedopusti/expluatacia/index.php?ELEMENT_ID=833)

Даже при неглубоком поиске в сети Интернет легко обнаружить сайты, где положительно оцениваются такие социально опасные явления, как сатанизм, сектантство, расовая и национальная нетерпимость, педофилия, различные виды сексуальных извращений, наркотизм и т.п. Отмечается появление сайтов, принадлежащих организованным преступным группировкам и террористическим организациям, через которые они не только обмениваются информацией, но и пытаются пропагандировать свои идеи и образ жизни. Молодые люди с неустоявшейся психикой при посещении подобных сайтов могут активно воспринять пропагандируемые здесь взгляды и перенести их в свою повседневную жизнь. Сетевые технологии усиливают процесс опосредованного общения людей, участники которого чаще всего имеют поверхностные, неглубокие межличностные отношения. Возникающие здесь контакты часто носят суррогатный, неполнценный характер. Это ведет к сокращению влияния ближайшего окружения на личность подростка как средства социального контроля, нарушению механизмов детерминации позитивного поведения. Более того, возможность анонимного участия в сетевом общении нередко формирует у молодых людей представление о вседозволенности и ненаказуемости любых проявлений в сетевой среде (Андреев Б.В., Пристанская О.В. и др. Информационные технологии в расследовании преступлений, совершенных с использованием сотовой связи. Научно-методическое пособие. Библиотека прокурора. Академия Генеральной прокуратуры Российской Федерации, М. 2009).

Чаще всего несовершеннолетние пользователи попадают на опасные странички случайно. Многочисленные всплывающие окна, неверно истолкованные поисковиком запросы, ссылки в социальных сетях – все это приводит ребенка на сайты небезопасного содержания, связанные с негативным контентом, киберхулиганством, домогательствами, виртуальными контактами с кибормошенниками, наркодилерами, экстремистами, педофилами, сутенерами и

порнографами

(http://www.detivrunete.ru/nedopusti/expluatacia/index.php?ELEMENT_ID=840) Значительное большинство подобных преступлений остаются скрытыми от родителей, правоохранительных органов и общества.

Исследования показали, что 90% детей сталкивались в сети с порнографией, а 65% искали ее целенаправленно. При этом 44% несовершеннолетних пользователей Интернета хотя бы раз подвергались в сети сексуальным домогательствам.

По данным главы МВД РФ Рашида Нургалиева «за последние годы количество сайтов с детской порнографией увеличилось почти на треть», а объём соответствующего контента вырос в 25 раз. В Интернете противоправные материалы такого рода предоставляют 300 млн. сайтов при среднемесячной посещаемости одной веб-страницы 30 тыс. человек. Число конечных потребителей, регулярно покупающих порнопродукцию с участием детей, оценивается в 800 тыс. человек ([Глава МВД РФ озабочен распространением в Интернете детской порнографии](#). — Interfax, 17 февраля 2010 года).

По данным Международного центра помощи пропавшим и эксплуатируемым детям (International Centre for Missing & Exploited Children), каждый седьмой ребёнок становится объектом сексуального домогательства в сети, причем, 4% являются объектом агрессивного домогательства, у 2% из них травмируется психика, к 4% детей злоумышленники обращаются с просьбами прислать свои фотографии, где они сняты полностью обнаженными или в сексуально откровенном виде. Объектами домогательств в сети в 70% становятся девочки, в 30% – мальчики. 81% подвергшихся таким домогательствам несовершеннолетних – подростки в возрасте от 14 лет и старше, на них же приходится 74% случаев психического травмирования.

Среди преступников, совершающих сексуальные домогательства в отношении несовершеннолетних в сети, 73% составляют мужчины, 16% – женщины, 5% выдавали себя за подростков. Большинство знакомится с детьми в чатах в целях совращения несовершеннолетних и последующей их сексуальной эксплуатации. Общение таких лиц в сети с детьми используется для установления доверительных отношений с ребенком, выработка уверенности в себе, вовлечения детей в разговоры на сексуальные темы, устроства личных встреч и интимных свиданий с потенциальными жертвами.

Особую озабоченность мирового сообщества вызывает распространение посредством сети Интернет, мобильных сетей **детской порнографии** (см., например, Е.И. Беспалов. Детская порнография: индустрия насилия. М., Дружественный Рунет, 2010).

По данным ЕСРАТ (международной организации по борьбе с детской порнографией), общий объем предложений детской порнографии возрос многократно, что обусловлено простотой и доступностью использования современной цифровой фото и видеотехники. Оборот детской порнографии относится к одному из самых быстрорастущих видов бизнеса в «Интернете», доступ к нему лёгок как никогда, так как расплачиваться можно с помощью кредитных карт, электронных и других платёжных средств. По состоянию на 2003 г. примерно 200.000 сайтов извлекали прибыль из оборота детской порнографии, оцениваемую в 3 млрд. долларов при очень невысокой ее себестоимости (Международное сотрудничество в сфере противодействия торговле детьми и детской порнографии. Материалы международной научно-практической конференции. Москва. 12-15 ноября 2008 г. – М. 2008).

В последние годы специалистами отмечается неблагоприятная тенденция снижения возраста детей, используемых преступниками для изготовления детской порнографии, и применения к жертвам все более жестоких, изощренных способов обращения в целях удовлетворения извращенных сексуальных потребностей и чудовищных сексуальных фантазий взрослых пользователей сети. Вскрываются факты совершения в формате он-лайн сексуального насилия и совращения в отношении несовершеннолетних и малолетних детей по предварительному заказу клиентов – пользователей.

У 83% задержанных владельцев детской порнографии были изъяты изображения детей в возрасте от 6 до 12 лет, у 39% - от 3 до 5 лет, у 19% - до 3 лет и даже грудных младенцев. У 21% порнографические материалы изображали сцены насилия, в том числе изнасилование, связывание конечностей и пытки; у 39% были движущиеся изображения в цифровой форме или в видеоформате. Среди задержанных владельцев детской порнографии: у 62% были изображения девочек; у 14% были изображения мальчиков; у 15% изображения девочек и мальчиков присутствовали в одинаковом количестве.

Опасность детской порнографии состоит также в ее использовании для вовлечения в секс- и порнобизнес все новых несовершеннолетних жертв. Для того чтобы «приручить» новых жертв, преступники показывают им порнографические изображения детей, где те якобы выглядят довольными, что снижает порог преодоления запрета у ребенка и снижает его восприимчивость. Они убеждают детей в том, что изображённые в порнографии дети участвуют в ней добровольно и с удовольствием, это помогает им стимулировать сексуальную активность

потенциальных жертв и облегчает встречу с ними (Детская порнография: модель законодательства и всемирный обзор. Copyright © 2008, Международный центр помощи пропавшим и эксплуатируемым детям (International Centre for Missing & Exploited Children)).

Для сведения. Во всем мире производство и оборот детской порнографии рассматривается как уголовное преступление, направленное против детей. Специальное законодательное регулирование борьбы с детской порнографией существует в 91 государстве из 187 государств – членов Интерпола.

В правовых системах некоторых стран только производство детской порнографии является преступлением, в ряде других, прежде всего, в англоязычных государствах, ее приобретение и хранение даже без цели последующего распространения тоже считаются уголовными преступлениями, как действия, содействующие виктимизации детей, облегчающие их сексуальную эксплуатацию, стимулирующие спрос на такую продукцию, формирующие в обществе аномальные представления о допустимости и нормотипичности сексуальных контактов взрослых с несовершеннолетними.

В России с 2003 года установлена уголовная ответственность за изготовление, хранение или перемещение через Государственную границу Российской Федерации в целях распространения, публичной демонстрации или рекламирования либо распространение, публичная демонстрация или рекламирование материалов или предметов с порнографическими изображениями несовершеннолетних, а равно привлечение несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера лицом, достигшим восемнадцатилетнего возраста. Совершение таких действий родителем или иным лицом, на которое законом возложены обязанности по воспитанию несовершеннолетнего, а равно педагогом или другим работником образовательного, воспитательного, лечебного либо иного учреждения, обязанным осуществлять надзор за несовершеннолетним, либо в отношении лица, не достигшего четырнадцатилетнего возраста, либо группой лиц по предварительному сговору или организованной группой, либо с извлечением дохода в крупном размере влечет более строгие меры наказания (ст. 242.1 Уголовного кодекса Российской Федерации – далее УК РФ).

Предусмотрена также уголовная ответственность за незаконные изготовление в целях распространения или рекламирования, распространение, рекламирование порнографических материалов или предметов, а равно незаконную торговлю печатными изданиями, кино-

или видеоматериалами, изображениями или иными предметами порнографического характера (ст. 242 УК РФ).

2.4. Виды он-лайн угроз, представляющих опасность для жизни, физического, психического и нравственного здоровья и полноценного развития ребенка

1. Самая распространенная угроза для детей в Интернете, это обилие *откровенных материалов сексуального характера*.

Многочисленные видеоролики и снимки с так называемой «жесткой эротикой», в том числе содержащие информацию о сексуальных извращениях, могут дезориентировать ребенка, ранить его психику, вызвать нарушения психосексуального и нравственно-духовного развития, воспрепятствовать построению нормальных социальных, в том числе межполовых и семейных отношений в будущем.

Интернет зачастую дает неверное представление о сути интимных отношений между людьми, эксплуатирует и извращает естественное любопытство детей, пользуясь несформированностью их психики и личностной системы ценностно-нормативных ориентаций.

К сожалению, в информационно-телекоммуникационных сетях куда больше материалов об извращенных формах секса, чем научно-популярной информации о взаимоотношениях полов. Ребенку особенно опасно сталкиваться с такими материалами до того, как будет сформирована их личность. Именно с опасностью неверного истолкования модели сексуального поведения людей связана другая угроза – ребенок может стать жертвой педофилов и порнографов, даже не подозревая о том, что его новые знакомые просят сделать что-то непристойное, например, раздеться в режиме он-лайн, ведь он видел, что в Интернете «все так делают».

Поэтому крайне важно, чтобы ребенок доверял родителями и педагогами и был подготовлен ими к восприятию и адекватной оценке той информации о взаимоотношениях полов, которую он может получить из Сети (http://www.detivrunete.ru/nedopusti/expluatacia/index.php?ELEMENT_ID=840)

2. При общении в Сети у каждого обязательно появляются *виртуальные знакомые и друзья*. Подобные отношения многим кажутся безобидными, поскольку Интернет-друг является как бы «ненастоящим»

и не может принести реального вреда. Однако это не так. Кроме своих сверстников и интересных личностей, общение с которыми пойдет на пользу, ребенок может завязать знакомство не только с педофилом и извращенцем, но и с мошенником и хулиганом. Виртуальное хамство и розыгрыши часто заканчиваются киберпреследованием и киберунизением, доставляя объекту травли множество страданий. Для ребенка такие переживания могут оказаться критичными, поскольку он более раним, чем взрослые люди.

Различия киберпреступлений от традиционных реальных преступных посягательств обусловлены особенностями интернет-среды: анонимностью, возможностью фальсификации, наличием огромной аудитории, возможностью достать жертву в любом месте и в любое время (http://www.detivrunete.ru/nedopusti/expluatacia/index.php?ELEMENT_ID=840).

В последние годы получили распространение такие общественно опасные посягательства на личность несовершеннолетнего в сети, как **кибербуллинг** (cyberbullying) – подростковый виртуальный террор, получил свое название от английского слова bull — бык, с родственными значениями: агрессивно нападать, бередить, задирать, придиরаться, провоцировать, донимать, терроризировать, травить. В молодежном сленге является глагол аналогичного происхождения — быковать.

Кибербуллинг — это нападения с целью нанесения психологического вреда, которые осуществляются через электронную почту, сервисы мгновенных сообщений, в чатах, социальных сетях, на web-сайтах, а также посредством мобильной связи. Такое многократно повторяемое агрессивное поведение имеет целью навредить человеку и базируется на дисбалансе власти (физической силы, социального статуса в группе) (<http://www.staysafeonline.org/in-the-home/cyberbullying-harassment-and-hacking>).

Наиболее опасными видами кибербуллинга считаются **киберпреследование** — скрытое выслеживание жертвы с целью организации нападения, избиения, изнасилования и т.д., а также **хеппислепинг** (Happy Slapping — счастливое хлопанье, радостное избиение) — видеоролики с записями реальных сцен насилия. Эти ролики размещают в интернете, где их могут просматривать тысячи людей, без согласия жертвы. Начинаясь как шутка, хеппислепинг может закончиться трагически. Название «хеппислепинг» происходит от случаев в английском метро, где подростки избивали прохожих, тогда как другие записывали это на камеру мобильного телефона

(http://www.detivrunete.ru/nedopusti/expluatacia/index.php?ELEMENT_ID=840)

Взрослые пока мало задумываются об опасностях обширной кибер-практики своих детей, хотя о последствиях буллинга реального приходится слышать часто: сообщения о травмах, нанесенных сверстниками, попытки суицидов и трагические смерти. Кибербуллинг остается невидимым, а нанесенный им ущерб — нераспознанным. Но вполне реальным, несмотря на виртуальность этой проблемы.

Встречается в виртуальной среде и так называемый *буллицид* – доведение ребенка до самоубийства путем психологического насилия (http://www.detivrunete.ru/nedopusti/expluatacia/index.php?ELEMENT_ID=840)

Порой киберпреследование имеет печальный финал (<http://cyberpsy.ru/2011/03/lyubov-najdenova-kiberbullying-opasnoe-virtualnoe-bykovanie/>)

Для безопасности несовершеннолетнего особую угрозу представляют личные встречи с виртуальными знакомыми в реальной жизни, о которых родители могут ничего не знать (http://rfdeti.ru/catalog/main_news/admin/upload/1270470934_memorandum.pdf).

Ребенку необходимо объяснить правила безопасного общения в сети (http://rfdeti.ru/catalog/main_news/admin/upload/1270470934_memorandum.pdf, http://www.detivrunete.ru/nedopusti/expluatacia/index.php?ELEMENT_ID=535, <http://www.staysafeonline.com/>, <http://www.staysafeonline.org/in-the-home/protect-yourself>).

3. Опасная для детей информация, способная причинить серьезный вред их здоровью, развитию и безопасности может содержаться *на электронных ресурсах, содержащих материалы экстремистского и террористического характера*.

Для сведения. Запрещается использование сетей связи общего пользования для осуществления экстремистской деятельности, на территории Российской Федерации запрещаются распространение экстремистских материалов, а также их производство или хранение в целях распространения. В случаях, предусмотренных законодательством Российской Федерации, производство, хранение или распространение экстремистских материалов является правонарушением и влечет за собой ответственность (ст. 12, 13 Федерального закона от 25.07.2002 № 114-ФЗ "О противодействии экстремистской деятельности").

Законом запрещены также возбуждение социальной, расовой, национальной или религиозной розни; пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии; пропаганда и публичное демонстрирование нацистской атрибутики или символики либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения; публичные призывы к осуществлению указанных деяний либо массовое распространение заведомо экстремистских материалов, а равно их изготовление или хранение в целях массового распространения (ст. 1 Федерального закона "О противодействии экстремистской деятельности").

4. Особую опасность представляют для незрелой психики несовершеннолетних *электронные ресурсы, созданные и поддерживаемые деструктивными религиозными sectами.*

Определить, особенно ребенку, сектантский ли сайт, который встретился ему в сети, очень трудно – иногда для того, чтобы понять, что этот сайт принадлежит секте, приходится проводить целые расследования. Как правило, это касается сайтов для родителей и их детей, сайтов про административные технологии в бизнесе, сайты по психологической консультации и проч. Подавляющее большинство лидеров сект любыми путями стремятся присутствовать в Интернете и рекламировать свою деятельность, предоставляя ложную информацию о себе. Главная проблема деструктивных сект в сети – это предоставление ложной информации. Попасть под негативное влияние секты через сайт очень легко – если ребенок читает в сети соответствующий материал, смотрит видео и фото-информацию, то он уже вступает во взаимодействие с вербовщиком секты, невольно участвует в психологической игре организаторов секты, нередко попадая от них в зависимость. Сектанты всегда вербуют новых адептов через интерес, так что если сайт интересен, кажется важным для несовершеннолетнего пользователя и весьма актуальным в его жизненных обстоятельствах – не исключено, что этот сайт может быть сектантским. Всегда надо проверять и перепроверять полученную информацию. И в этом может помочь специальная религиоведческая литература и соответствующая справочная и информационно-аналитическая информация в Интернете (http://saferunet.ru/ruaos/stories/detail.php?SECTION_ID=143&ID=970, <http://spisok-sekt.ru/>).

Для сведения. Вовлечение малолетних в религиозные объединения, а также обучение малолетних религии вопреки их воле и без согласия их родителей или лиц, их заменяющих, запрещены (ст. 3

Федерального закона от 26.09.1997 № 125-ФЗ "О свободе совести и о религиозных объединениях"). Запрещается также создание и деятельность религиозных объединений, цели и действия которых противоречат закону (ст. 6 указанного Федерального закона).

5. Доверчивость и наивность детей нередко используют в своих целях компьютерные **мошенники, спамеры, фишеры**. Несовершеннолетние нередко переходят по присланным им злоумышленниками ссылкам без подозрений, скачивают неизвестные файлы, которые могут оказаться вирусами или содержать незаконную информацию.

Недостаточно информированный об опасностях в сети ребенок может сообщить злоумышленнику номер кредитной карточки родителей, пароль от электронного кошелька, свой настоящий адрес и многое другое (<http://www.staysafeonline.org/in-the-home/spam-and-phishing>).

Несовершеннолетнего пользователя взрослые преступники могут с использованием электронных ресурсов втянуть *в совершение антиобщественных, противоправных, в том числе уголовно-наказуемых деяний*. При этом следует иметь в виду, что привлечение к уголовной ответственности взрослого лица за вовлечение несовершеннолетнего в совершение преступления не исключает уголовной ответственности и самого подростка в случаях, когда он достиг установленного уголовным законом возраста.

По мнению психологов, анонимность и отсутствие запретов освобождают скрытые комплексы (в первую очередь, связанные с тягой к насилию и сексуальностью), стимулируют людей переходить некоторые нравственные границы. Есть немало примеров, когда подростки используют сетевые возможности, чтобы досаждать людям, с которыми в реальной жизни их связывают неприязненные отношения. Злоумышленник в таком случае преследует жертву, направляя ей угрозы с помощью сетевых средств. Подобные факты зафиксированы и в отечественной правоохранительной практике. Сетевая среда способна оказывать определенное влияние и на психическое здоровье личности.

Известны случаи вовлечения подростков через Интернет:

- в действия, носящие оскорбительный (статья 130 УК РФ «Оскорбление») и клеветнический характер (статья 129 УК РФ «Клевета»);
- в экстремистскую деятельность (статья 282 УК РФ «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства»; статья 282.1 «Организация экстремистского сообщества»;

статья 282.2 «Организация деятельности экстремистской организации»; статья 239 «Организация объединения, посягающего на личность и права граждан»);

– в преступную деятельность по изготовлению и сбыту наркотических средств и психотропных веществ и склонению к их потреблению несовершеннолетних (статьи 228, 228.1, 230 УК РФ), незаконному обороту оружия, взрывных устройств и взрывчатых веществ (статья 222 «Незаконные приобретение, передача, сбыт, хранение, перевозка или ношение оружия, его основных частей, боеприпасов, взрывчатых веществ и взрывных устройств», статья 223 «Незаконное изготовление оружия»), сильнодействующих или ядовитых веществ в целях сбыта (ст. 234 УК РФ);

– в секс- и порнобизнес, включая незаконное распространение порнографических материалов и предметов (статья 242), изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних (статья 242.1), вербовку несовершеннолетних сверстников (сверстниц) в занятие проституцией (статья 240 «Вовлечение в занятие проституцией»; статья 241 УК РФ «Организация занятия проституцией») и другие виды преступлений.

Ребенку следует объяснить, что указанные общественно опасные деяния, независимо от того, совершаются ли они с применением традиционных способов и средств или с использованием информационно-телекоммуникационных сетей, уголовно наказуемы, в том числе для подростков, достигших установленного законом возраста уголовной ответственности (16 лет, а за отдельные виды преступлений – с 14 лет в соответствии со статьей 20 УК РФ).

Для сведения. Действия совершеннолетнего лица (достигшего 18-летнего возраста), вовлекшего, в том числе с использованием интернета или мобильной связи, несовершеннолетнего в совершение преступления или антиобщественного действия (в систематическое употребление спиртных напитков, одурманивающих веществ, в занятие бродяжничеством или попрошайничеством), склонившего ребенка или подростка к потреблению наркотических средств или психотропных веществ, уголовно наказуемы (статьи 150, 151, 230 УК РФ).

6. Пропаганда наркотиков, насилия и жестокости, суициdalного поведения, абортов, самоповреждений может быть весьма опасной для неокрепшей детской психики. Ребенок на веру принимает многие сомнительные идеи, особенно если они грамотно изложены. Например, о том, как лучше покончить с собой или от приема каких таблеток «станет веселее», как без обращения к врачу избавиться

от нежеланной беременности и т.д. Этим пользуется немало людей, использующих детей в корыстных и иных личных целях. Согласно Конвенции ООН о правах ребенка такие действия есть не что иное, как **кriminalная, в том числе коммерческая эксплуатация ребенка**.

Для сведения. Пропаганда насилия и жестокости, порнографии, в том числе в средствах массовой информации и рекламе, запрещена российским законодательством (ст. 4 Закона РФ от 27.12.1991 № 2124-1 "О средствах массовой информации", ст. 31, "Основы законодательства Российской Федерации о культуре" (утв. ВС РФ 09.10.1992 № 3612-1), ст. 5 Федерального закона от 13.03.2006 № 38-ФЗ "О рекламе").

В Российской Федерации **запрещены** также:

- распространение в средствах массовой информации, а также в информационно-телекоммуникационных сетях сведений о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров;
- пропаганда каких-либо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров, а также распространение иной информации, распространение которой запрещено федеральными законами (ст. 4 Закона РФ от 27.12.1991 № 2124-1 "О средствах массовой информации");
- производство и распространение книжной продукции, продукции средств массовой информации, распространение указанных сведений посредством использования информационно-телекоммуникационных сетей или совершение иных действий в этих целях (статья 46 Федерального закона от 08.01.1998 № 3-ФЗ (ред. от 06.04.2011) "О наркотических средствах и психотропных веществах").

За совершение указанных деяний установлена административная ответственность (ст. 6.13 Кодекса Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ).

Для сведения. В случаях, когда такая пропаганда носит признаки склонения несовершеннолетнего к потреблению наркотических средств и психотропных веществ, виновный, достигший шестнадцатилетнего возраста, привлекается к уголовной ответственности по статье 230 УК РФ, предусматривающей за такие действия наказание на срок от шести до двенадцати лет.

7. Помимо указанной выше информации в Сети есть **немало сомнительных развлечений, таких как онлайн-игры,**

пропагандирующие секс, жестокость и насилие, требующие немалых финансовых вложений. Дети бывают вовлечены в азартные игры в сети.

Онлайн-игры играют значительную роль в жизни современных детей и подростков. Для многих они становятся важной составляющей повседневности, определяют стиль, круг общения, влияют на жизненные ценности (и сами становятся ценностью, а нередко и сверхценностью). В результате увлечения играми ребенок может сильно снизить успеваемость в школе, прекратить заниматься социально полезными видами деятельности, сократить до минимума время, проводимое с родными и реальными друзьями, полностью переключиться на виртуальные формы общения и досуга, то есть приобрести Интернет-зависимость, которую многие психологи склонны считать болезнью.

Особого внимания требует предупреждение влияния на установки личности ребенка распространенных в глобальных сетях игр с элементами насилия. Исследования показали, что жестокие игровые эпизоды нередко приводят к нарастанию агрессивности поведения несовершеннолетних. Очевидно, с развитием технологий указанная проблема будет только усложняться, поскольку компании-разработчики игр постоянно повышают качество соответствия игрового пространства реальности, а это ведет к возрастанию степени погружения личности в виртуальную среду.

Для того чтобы снизить риски негативного воздействия компьютерных и электронных игр на несовершеннолетних, культуре общения в онлайн-играх, правилам безопасной игры детей и подростков необходимо специально обучать (http://rfdeti.ru/catalog/main_news/admin/upload/1270470934_memorandum.pdf), а также предпринимать соответствующие меры по обеспечению безопасности ребенка при выборе игры (<http://www.pegi.info/en/index/>).

В соответствии с п. 3 ст. 14 Закона об основных гарантиях прав ребенка в целях обеспечения безопасности жизни, охраны здоровья, нравственности ребенка, защиты его от негативных воздействий предусмотрено проведение экспертизы (социальной, психологической, педагогической, санитарной) предназначенных для детей: настольных, компьютерных и иных игр, игрушек и игровых сооружений. С учетом сложившейся в экспертной практике и закрепленных в законодательстве субъектов РФ критериев их безопасности для нравственного, психического здоровья и нормального развития детей среди несовершеннолетних не допускается распространение игр, в том числе компьютерных и электронных, и игрушек: 1) провоцирующих ребенка на агрессивные действия; 2) вызывающих у него проявление жестокости по отношению к персонажам игры, в роли которых выступают

играющие партнеры (сверстники, взрослые) или сама сюжетная игрушка; 3) провоцирующих игровые сюжеты, связанные с безнравственностью и насилием; 4) вызывающих преждевременный и нездоровий интерес к сексуальным проблемам, не соответствующий возрастным потребностям ребенка; 5) провоцирующих ребенка на пренебрежительное или негативное отношение к расовым особенностям и физическим недостаткам других людей. Любой из указанных критериев в отдельности достаточно, чтобы признать игру (игрушку) вредной для здоровья и развития детей и подростков.

Для сведения. В России собственная рейтинговая система оценки, классификации и маркировки компьютерных и электронных игр в настоящее время отсутствует. Введение такой системы ожидается после вступления в силу с 1 сентября 2012 года федеральных законов № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" и № 252-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О защите детей от информации, причиняющей вред их здоровью и развитию". Согласно указанным законам любая информация, размещаемая в информационно-телекоммуникационных сетях (в том числе в сети Интернет) и сетях подвижной радиотелефонной связи, подлежит возрастной классификации и маркировке знаками, соответствующими определенной возрастной категории потребителей, для которых предназначена соответствующая информационная продукция. Нарушение указанного требования будет влечь административную ответственность.

В мире существует множество различных методов оценки контента видео- и компьютерных игр, а также их возрастной классификации и маркировки. Наиболее распространенными являются две рейтинговые системы – PEGI и ICRA.

Резолюция Совета ЕС 2002 г. о защите молодых людей от неприемлемого материала в видео и компьютерных играх (Council Resolution on the protection of consumers, in particular young people, through the labelling of certain video games and computer games according to age group, 1 March 2002 (OJ C 65, 14.3.2002, p. 2) подчеркивает необходимость предоставления потребителям, в том числе юным, четкой информации о приемлемости контента для определенных возрастных групп путем определения возрастной категории видео и компьютерных игр и их маркировки. Ясная и простая система возрастной классификации должна применяться во всех государствах-членах ЕС для обеспечения прозрачности и свободного распространения

видео игр. Совет подчеркнул важность сотрудничества заинтересованных сторон.

Система рейтинга сайтов **ICRA** была построена на базе уже существующей RSACi, является результатом усилий многих мировых компаний. ICRA — Internet Content Rating Association или Ассоциация рейтинга содержимого Интернета — независимая, некоммерческая система рейтинга сайтов, основанная весной 1999 года группой ведущих мировых интернет-компаний и ассоциаций.

Цель ICRA — разработать, внедрить и управлять международными системами рейтинга информации, позволяющими пользователям по всему миру ограничить доступ к сайтам, содержимое которых может нанести моральный урон, в особенности детям.

PEGI — европейская рейтинговая система компьютерных и видеоигр и другого развлекательного программного обеспечения. Разработана Европейской федерацией интерактивного программного обеспечения и начала работу в апреле 2003 года. Поддерживается Европейской Комиссией, хотя и не находится под управлением Евросоюза (www.pegi.info).

Рейтинг состоит из двух частей - оценки возрастных ограничений для продукта, а также от одного до семи описаний содержимого, которые предупреждают о ненормативной лексике, насилии и т. п.

Для сведения, используемые PEGI логотипы описаний:



Bad Language - Ненормативная лексика
Игра содержит грубые и непристойные выражения.



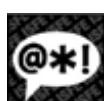
Discrimination - Дискриминация
Присутствие в продукте сцен или материалов, которые могут порочить или дискриминировать некоторые социальные группы.



Drugs - Наркотики
В игре упоминаются нелегальные наркотические вещества или пропагандируется их использование.



Fear - Страх:
Материалы игры могут оказаться страшными и пугающими для маленьких детей.



Gambling - Азартные игры
В игре есть возможность сыграть в азартные игры и сделать ставку, в том числе — реальными деньгами.



Sexual Content – Непристойности

В игре присутствует обнажение и/или встречаются сцены с сексуальными отношениями.



Violence - Насилие

Игра изобилует сценами с применением насилия.

Информация о рейтинге игр (с указанием видов вредного контента и возрастной классификации) печатается на упаковке игры, содержится в ее рекламе и указывается на сайте игры. Возрастная категория и краткие описания присутствуют на упаковке продукта в виде логотипов.

Возрастные категории 16+ или 18+ тщательно проверяются перед тем, как получить рейтинг, а 12+, 3+ и 7+ – уже после присвоения им рейтинга. В завершение процесса возрастной классификации NICAM выдает от лица Европейской федерации интерактивного программного обеспечения (ISFE) лицензию на право использования логотипа и описания данного товара.

Систему PEGI поддерживают большинство производителей игровых консолей. Она используется для возрастной классификации и маркировки большинства видеоигр в 25 европейских странах (Финляндия, Греция, Италия, Латвия, Нидерланды, Польша, Португалия, Словакия, Великобритания, Франция, Бельгия, Болгария, Дания, Эстония, Венгрия, Ирландия, Испания, Швеция, Чешская Республика и др.).

Следует также обратить внимание на профилактику *случаев вовлечения несовершеннолетних в азартные игры, организуемые в виртуальных сетях*.

Для сведения. Деятельность по организации и проведению азартных игр с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет, а также средств связи, в том числе подвижной связи, а равно посещение игорных заведений лицами, не достигшими возраста восемнадцати лет, запрещены действующим законодательством (Федеральный закон от 29.12.2006 № 244-ФЗ "О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации", ст. 5, ч. 2 ст. 7).

8. Психологами отмечается распространность в среде пользователей, в том числе несовершеннолетних, случаев *болезненного пристрастия к участию в сетевых процессах, так называемой "Интернет-зависимости"*, проявляющегося в навязчивом желании

неограниченно долго продолжать сетевое общение <http://psygrad.ru/slovar/i/internet-zavisimost.html>. По данным различных исследований, интернет-зависимыми сегодня являются около 10 % пользователей во всём мире.

Нередко несовершеннолетние настолько привязываются к виртуальному миру и своему вымышленному персонажу, что забывают обо всем остальном. Для подростков Интернет, как виртуальная среда иногда кажется даже более адекватной, чем реальный мир. Возможность перевоплотиться в некую бестелесную "идеальную личность" открывает для них новые ощущения, которые им хочется испытывать постоянно или все более часто.

Зависимость (аддикция) в психологии определяется как навязчивая потребность, ощущаемая человеком, подвигающая к определённой деятельности. Этот термин употребляется не только для определения наркомании, но и применяется к другим областям, типа проблемы азартных игр и интернет-зависимости. Специалисты отмечают, что в некоторой степени указанная зависимость близка к патологической увлеченности азартными играми, а ее деструктивные эффекты схожи с возникающими при алкоголизме и наркомании, однако, в отличие от последних, имеют нехимическое происхождение.

Высказывается мнение, что в подавляющем большинстве случаев такая зависимость – не самостоятельное состояние, а синдром в рамках другого психического расстройства (http://saferunet.ru/ruaos/stories/detail.php?SECTION_ID=143&ID=949).

Таким образом, Интернет-зависимость (как вид нехимической зависимости) – это навязчивая потребность в использовании Интернета, сопровождающаяся социальной дезадаптацией и выраженными психологическими симптомами <http://inaddiction.narod.ru/3.html>. Патология проявляется в разрушении обычного образа жизни, смене жизненных ориентиров, появлении депрессии, нарастании социальной изоляции. Происходит социальная дезадаптация, нарушаются значимые общественные связи.

Выделяется 6 основных типов интернет-зависимости с учетом того, к чему сформировалось пристрастие у конкретной личности: "киберсексу", виртуальным знакомствам, сетевым азартным играм, компьютерным играм или навязчивому перемещению по Web-узлам (<http://www.psylines.ru/inzav.htm>):

1. Навязчивый веб-серфинг — бесконечные путешествия по Всемирной паутине, поиск информации.

2. Пристрастие к виртуальному общению и виртуальным знакомствам — большие объёмы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в Сети.
3. Игровая зависимость — навязчивое увлечение компьютерными играми по сети.
4. Навязчивая финансовая потребность — игра по сети в азартные игры, ненужные покупки в интернет-магазинах или постоянные участия в интернет-аукционах.
5. Пристрастие к просмотру фильмов через интернет, когда больной может провести перед экраном весь день, не отрываясь из-за того, что в сети можно посмотреть практически любой фильм или передачу.
6. Киберсексуальная зависимость — навязчивое влечеение к посещению порносайтов и занятию киберсексом.

О клиническом феномене зависимости от игр и ПК (лудомания, игромания, гэмблинг) говорят с конца 1980-х годов, сначала за рубежом, теперь, по мере продвижения информационных технологий, и в России.

Основные признаки **Интернет-зависимости**: 1) чрезмерное, немотивированное злоупотребление длительностью работы в сети, не обусловленное профессиональной, учебной или иной созидательной деятельностью; 2) использование Интернета как преобладающего средства коммуникации; 3) создание и эксплуатация виртуальных образов, крайне далеких от реальных; 4) влечеение к Интернет-играм и(или) созданию вредоносных программ (без какой-либо цели); 5) субъективно воспринимаемая невозможность обходиться без работы в сети (http://saferunet.ru/ruaos/stories/detail.php?SECTION_ID=143&ID=949).

При появлении указанных выше признаков следует обратиться за медицинской (психологической и(или) психиатрической помощью, так в запущенном состоянии Интернет-зависимость и игромания значительно хуже поддаются коррекции.

9. Опасность для детей представляют также *социальные сети и блоги, на которых ребенок оставляет о себе немало настоящей информации, завязывает небезопасные знакомства, нередко подвергается незаметной для него деструктивной психологической и нравственно-духовной обработке*.

Социальные сети стали пользоваться популярностью несколько лет назад, так как, во-первых, удовлетворяют потребность интернет-пользователей в коммуникациях и социализации, а, во-вторых, —

открывают простор для творчества и самовыражения (функционал позволяет создавать и публиковать контент самостоятельно и без премодерации).

Пользователи социальных сетей (как всемирных, так и русскоязычных) могут общаться друг с другом в киберпространстве, выкладывать фотографии и видео, делиться со своими друзьями ссылками на интересный по той или иной причине контент, обмениваться виртуальными подарками и так далее. В Рунете наблюдался колоссальный рост активности пользователей благодаря социальным сетям Odnoklassniki.ru и Vkontakte.ru. В целом, с ростом популярности блогосферы и социальных сервисов Интернет вошел в новую, Web 2.0-эпоху, когда пользователи являются не столько потребителями информации, сколько её создателями, причем активными.

Массовость и бурный рост социальных сетей повлекли за собой и целый ряд негативных последствий, среди которых – *появление новых форм киберпреступлений: от мошеннических махинаций и нарушений авторских прав до распространения детской порнографии, пропаганды педофилии, торговли детьми.*

Злоумышленникам особенно легко искать своих несовершеннолетних жертв с помощью таких сайтов как «Вконтакте», «Одноклассники» и «Мой мир». Совершенно не стесняясь, педофилы создают свои группы и сообщества прямо в социальных сетях, выкладывают в открытый доступ фото и видео-материалы порнографического содержания.

На созданные несовершеннолетними пользователями в социальных сетях странички уже в течение 2-3 дней могут поступить как прямые непристойные предложения, так и сообщения от педофилов, входящих в доверие к детям и подросткам под видом сверстников и даже заводящих с ними дружеские отношения <http://www.ligainternet.ru/novosti>

10. Дети все чаще используются дельцами от порнобизнеса *в качестве моделей для детской порнографии* (http://www.detivrunete.ru/nedopusti/expluatacia/index.php?ELEMENT_ID=761)

Порнографический контент (в том числе, с участием несовершеннолетних) публикуется как в закрытых группах или сообществах, так и в открытом доступе – в зависимости от целей «автора» публикаций. Он появляется в социальной сети с «завидной» регулярностью: пользователи создают тематические группы и страницы, объединяются по соответствующим «интересам», публикуют десятки и

сотни видеороликов порнографического содержания, текстовые заметки и
и
(http://www.detivrunete.ru/nedopusti/expluatacia/index.php?ELEMENT_ID=761)

В августе 2009 года МВД России признало социальную сеть Vkontakte.ru основным хранилищем детской порнографии в российском сегменте Интернета. На ресурс «Вконтакте» пришлось больше половины такого рода контента, выявленного в ходе мероприятий органов правопорядка в Сети в этом году (870 страниц сети из 1409).

В сфере коммерческой сексуальной эксплуатации детей, в том числе с использованием новых информационных технологий, в стране отмечается крайне тревожная ситуация. Количество выявленных при участии Управления «К» правоохранительными органами фактов изготовления и распространения материалов с порнографическими изображениями несовершеннолетних возросло в 2009 г., по сравнению с 2008 г., на 59,6% (с 223 до 356), в 2010 г., по сравнению с 2009 г., – на 72,2% (с 356 до 613).

Подавляющее большинство из них – 92,8% (569 преступлений) совершены *с использованием сети Интернет*, что существенно повышает общественную опасность этого деяния, поскольку практически навсегда запечатлевает образ растленного ребенка в информационных ресурсах сети Интернет и провоцирует лиц с патологическим влечением к детям к совершению более тяжких преступлений педофильного характера.

По данным МВД России наблюдается рост расследуемых преступлений по статье 242.1 УК РФ (изготовление и оборот порнографических изображений с участием несовершеннолетних): только за первые три месяца 2011 года зарегистрировано 128 таких преступлений, что на 20 процентов выше показателей аналогичного периода прошлого года. В 2004 года таких преступлений было зарегистрировано 13, а в 2010 уже 569.

Подобрать себе жертву педофил может не только в детском чате или форуме. Ему вполне могут помочь абсолютно доступные Интернет-сайты школ, детских кружков и прочих внешкольных организаций, где публикуются списки и фотографии учащихся или кружковцев, а то и с расписаниями занятий по группам или классам. В результате педофил может точно установить местонахождение ребенка и по фотографии даже оценить объект "охоты". Дальше ребенка встречают у школы, обманывают какой-нибудь «легендой» и ведут в укромное место.

Главное средство защиты от педофила – ребенок должен твердо усвоить, что виртуальные знакомые должны оставаться виртуальными. То есть – никаких встреч в реальном мире с теми друзьями, которых он обрел в Интернете. По крайней мере, без родительского присмотра. Если в семье установлены отношения доверительные и ребенок не таит свою жизнь от родителей, он сам поведает о своих друзьях и контактах. Даже если речь идет о «партнерах по сетевой игре» – все равно встреча должна состояться «на своей территории» или под родительским наблюдением. Только убедившись в том, что из виртуальной среды на встречу с ребенком стремится не взрослый дядя с пошлыми и циничными намерениями, родитель может позволить такую встречу, желательно, под своим контролем.

(http://www.detivrunete.ru/nedopusti/expluatacia/index.php?ELEMENT_ID=538,
http://www.detivrunete.ru/nedopusti/expluatacia/index.php?ELEMENT_ID=539).

11. Дети нередко оказываются на ресурсах, имеющих содержание 18+, или участвуют в сетевой деятельности, совершенно не предназначенной для них, например, в виртуальном сексе.

Виртуальный секс – это использование различных Интернет-материалов (картинок, текстов, звуков, видео) для сексуального стимулирования и удовлетворения. Вероятность попасть на несовершеннолетнего партнера для виртуального секса крайне велика. Главной особенностью киберсекса является его доступность. Для того чтобы заняться им, достаточно найти нужный сайт. Все пользователи Сети, включая детей, в любое время дня и ночи дома, в офисе или интернет-клубе могут завести разговор с незнакомцем, который примет сексуальный уклон.

Анонимность позволяет сохранять тайну своей личности или выдавать себя за человека другого пола и возраста. Таким образом, не только педофилы могут притворяться кем-то другим, соблазняя детей, но и сами дети могут выдавать себя за взрослых для того, что «развлечься». На практике, больше половины посетителей чат-комнат «Виртуальный секс», младше 18 лет. Вопреки распространенному заблуждению о том, что сексом в Интернете интересуются только мальчики, несовершеннолетних посетительниц секс-чатов не намного меньше. Интересно, что во время общения, практически никто из них не признается собеседникам в своем настоящем возрасте. При этом те, кто позиционируют себя 13-летними подростками, чаще всего таковыми не являются и оказываются мужчинами старше 30 лет.

Виртуальное общение вовлекает детей и подростков в сексуальную активность, суть которой они не способны понять и оценить. Виртуальный секс, пережитый на ранней стадии жизни, может оказаться крайне негативное влияние на сексуальное развитие ребенка.

По данным современных психологических исследований, любители виртуального секса страдают от многих психологических расстройств. У 27% из них есть депрессия, 30% страдают от беспокойства, а 35% от стресса. Общение с такими людьми крайне нежелательно для ребенка, даже без учета сексуального подтекста. Ребенок, практикующий виртуальный секс, вскоре может захотеть испробовать его на практике, что повышает для него риск стать жертвой преступников-педофилов и порнографов. Посчитав развращенность нормой жизни, ребенок имеет высокий шанс стать объектом сексуальной эксплуатации (http://www.detivrunete.ru/nedopusti/expluatacia/index.php?ELEMENT_ID=538, http://www.detivrunete.ru/nedopusti/expluatacia/index.php?ELEMENT_ID=833).

Симптомами растления ребенка педофилем могут быть резкие изменения его поведения – ребенок становится замкнутым, плаксивым, боязливым, начинает плохо спать по ночам, а также лишние деньги, которых у детей обычно не бывает – частые «подарки» в сто (пятьсот, тысячу) рублей (обычно именно такими суммами подкупают ребенка злоумышленники). Вместо купюр могут наличествовать новые игрушки, одежда (родителями или родными не покупавшаяся), гаджеты (электронные игры или даже мобильник) (http://www.detivrunete.ru/nedopusti/expluatacia/index.php?ELEMENT_ID=540).

По исследованиям ГНЦССП имени В.П. Сербского, в числе психологических и клинических последствий непосредственных сексуальных контактов детей со взрослыми лицами у несовершеннолетних потерпевших встречаются: девиации поведения (агgressия, психопатоподобные и гипердинамические расстройства); снижение социального функционирования (школьная неуспешность, побеги из дома и школы, включение в асоциальные группировки); девиации психосексуального развития, формирование парафилий; посттравматические расстройства в форме психогенных невротических расстройств (энурез, логоневроз, страхи, астенодепрессивные состояния, атипичные депрессии, а также психосоматические и тревожно-фобические нарушения), личностных и психосексуальных расстройств (в виде опережения и извращения становления сексуальности, вплоть до

формирования садомазохистских тенденций с гомосексуальной ориентацией у мальчиков) и поведенческих нарушений, включая аффективные расстройства и агрессивные реакции, в том числе аутоагgression в виде членовредительства и суицидальных попыток, формирование гомосексуальной ориентации и промискуитетного поведения (беспорядочных половых связей).

К отдаленным последствиям, которые возникают по прошествии длительного времени, судебные сексологи относят такие, как: 1) проституция; 2) аномальная сексуальная активность в отношении своих детей в половозрелом периоде; 3) гомосексуальная ориентация; 4) расстройства сексуального влечения; 5) супружеская дезадаптация.

В научной литературе приводятся сведения, согласно которым сексуальным посягательствам в детстве были подвержены 21% пациентов с анорексией, 36% – с булимией и 33% – с иными психическими расстройствами.

Анонимный характер размещения информации в сети Интернет и сетях мобильной радиотелефонной связи, их интеграция, доступность и универсальность технических средств доступа к информационным ресурсам, сложность определения места фактического нахождения отдельных документированных материалов и установления их владельцев, наличие анонимных платежно-расчетных систем, – все это в совокупности привлекает повышенное внимание криминальных структур, способствуют распространению преступлений, совершаемых с использованием информационных технологий.

Жертвами таких преступлений нередко становятся несовершеннолетние и малолетние дети, доверием и неопытностью которых злоупотребляют взрослые преступники. Виртуальный и транснациональный характер электронной связи привел к тому, что общественно опасные посягательства на права и законные интересы несовершеннолетних в глобальной сети становятся все более серьезной проблемой, причем не только на внутригосударственном, но и на международном уровне.

12. Кроме преступлений против половой неприкосновенности несовершеннолетних и малолетних с использованием сети Интернет в отношении детей и подростков *совершаются также такие преступления, как похищение несовершеннолетнего, торговля несовершеннолетними, вовлечение несовершеннолетнего в занятие проституцией, организация занятия проституцией с использованием для занятия проституцией несовершеннолетних и малолетних потерпевших, а также преступления против собственности (компьютерные мошенничества)*.

В 2010 г. выявлено более 9,5 тыс. преступлений против половой неприкосновенности детей, установлено 23 факта торговли несовершеннолетними и 81 случай похищения ребенка. Сколько всего таких преступлений против несовершеннолетних совершено с использованием интернета и сетей мобильной (сотовой) связи, статистически не фиксируется.

С «улиц» и из притонов в виртуальное пространство Интернета перемещается и сутенерский бизнес, не брезгующий использованием в качестве живогоекс-товара детей (и это общемировая тенденция).

Для сведения. Вовлечение в занятие проституцией или принуждение к продолжению занятия проституцией, совершенные в отношении заведомо несовершеннолетнего (ст. 240 Уголовного кодекса Российской Федерации (далее – УК РФ), а также деяния, направленные на организацию занятия проституцией другими лицами, а равно содержание притонов для занятия проституцией или систематическое предоставление помещений для занятия проституцией, совершенные с использованием для занятия проституцией заведомо несовершеннолетних или лиц, заведомо не достигших четырнадцатилетнего возраста (ст. 241 УК РФ) относятся к категории тяжких и особо тяжких преступлений.

13. Не менее опасным является *совершение в отношении детей описанных выше общественно опасных посягательств с использованием мобильной (сотовой) связи.*

В числе потенциально опасной для несовершеннолетних информации в сети мобильной (сотовой) связи также анимированные фотографии, цветные картинки, открытки, иконки эротического содержания, ай-фри эротоны и модные звонки, содержащие «забористый мат, женский оргазм...» и другие непристойные звуки и высказывания, услуги «ай-фри мобильное видео» и «ай-фри мобильные книги», позволяющие детям и подросткам получить на свой мобильный телефон видеоролики порнографического содержания (в том числе посвященные однополой любви), бесплатные эротические игры, эротические истории, эро-гадания и т.п.

В распространяемых посредством сети мобильной связи типовых электронных сообщениях широко используются жаргонные и иные ненормативные слова и выражения, пропагандируются наркотики, алкоголепотребление, курение, сексуальные парофилии (извращения), насилие и жестокость.

Обеспечение медиабезопасности детей предполагает обязательное обучение их правилам безопасного пользования услугами мобильной

(сотовой) связи (<http://www.staysafeonline.org/in-the-home/mobile-devices>).

Для сведения. В подписанном 6 февраля 2007 года ведущими мобильными операторами Европы в Брюсселе Соглашении о защите несовершеннолетних пользователей мобильных телефонов предусмотрено принятие на основе саморегулирования таких мер, как контроль доступа только для взрослых; просветительские кампании для родителей и детей; классификация коммерческого содержания контента в соответствии с национальными стандартами приличия и уместности; борьба с незаконным содержанием на мобильных (сотовых) телефонах.

2.5. Государственные органы и общественные организации, занимающиеся проблемами защиты детей в киберпространстве

Управление «К» МВД России – подразделение в составе Бюро специальных технических мероприятий МВД РФ, занимающееся раскрытием преступлений в сфере высоких технологий. Образовано в 1998 году.

http://www.memoid.ru/node/Upravlenie_%C2%ABK%C2%BB_MVD_Rossii

Юрисдикция Управления «К» распространяется на следующие виды преступлений ([История создания и основные направления деятельности](#), материалы официального сайта МВД РФ):

- противоправные действия в сфере компьютерной безопасности (неправомерный доступ к информации, изготовление и распространение вредоносных программ, мошенничества с электронными платёжными системами, распространение в Интернете порнографических материалов с участием несовершеннолетних);
- преступления в информационно-телекоммуникационных сетях (нелегальный доступ к информации и незаконное использование ресурсов сетей сотовой и проводной связи, Интернета, спутникового и кабельного телевидения);
- незаконный оборот радиоэлектронных и специальных технических средств;
- нарушения авторских прав, изготовление и распространение нелицензированного программного обеспечения (ПО);

- международные преступления в сфере информационных технологий.

С 2009 года количество обращений граждан в Управление «К» МВД России возросло в 2 раза. Основной объем составляют заявления о фактах мошенничества и распространения детской порнографии. В 2010 году по материалам Управления «К» МВД России возбуждено более 12,5 тыс. уголовных дел, в том числе по фактам преступлений, совершенных в сети Интернет <http://www.mvd.ru/>.

Фонд Развития Интернет - <http://www.fid.su/>.

Целями создания Фонда являются: поддержка проектов, связанных с развитием сети Интернет; содействие развитию глобальных информационных сетей; содействие развитию правового обеспечения в Сети.

Фонд Развития Интернет открыл *интернет-сайт "Дети России Онлайн"* www.detionline.com, призванный обеспечить безопасное использование интернетом детьми. На сайте Фонд представляет свои основные проекты, посвященные вопросам социализации детей и подростков в развивающемся информационном обществе, а также проблемам их безопасности в современной инфокоммуникационной среде.

<http://www.positivecontent.ru/> 1 июня 2011 года, в День защиты детей, стартовал третий Всероссийский конкурс сайтов для детей и юношества "*Позитивный контент - 2011*"! Сайт конкурса: www.positivecontent.ru. Соорганизаторами "Позитивного контента" стали компания RU-CENTER, Фонд Развития Интернет и Hosting Community. Главные задачи этого конкурса - найти наиболее качественные, интересные, образовательные и безопасные (как в техническом, так и в контентном смысле) сайты; а также поддержать (и как следствие подтолкнуть к созданию новых) полезные и позитивные сайты, вовлекающие детскую и молодежную аудиторию Рунета в активную жизнь, как в Сети, так и за ее пределами. К участию в "Позитивном контенте - 2011" приглашены интернет-ресурсы для детей, подростков и молодежи, которые обладают познавательной, образовательной, информационной, коммуникационной или развлекательной направленностью.

<http://detionline.com/journal> *Журнал "Дети в информационном обществе"* – издательский проект, осуществляемый Фондом Развития Интернет с 2009 года при научной поддержке факультета психологии МГУ имени М.В. Ломоносова и Федерального института развития образования Министерства образования и науки РФ.

<http://detionline.com/research/about> Фонд Развития Интернет с 2007 года осуществляет всероссийские исследования по проблемам восприятия и использования ИКТ детьми и подростками, их социализации в развивающемся информационном обществе.

В настоящее время Фонд совместно с факультетом психологии МГУ имени М.В. Ломоносова и Федеральным институтом развития образования МОН РФ проводит всероссийское исследование "Дети России онлайн" в 12-ти регионах России на основе методологии проекта EU Kids Online II.

РОЦИТ – общественная организация российской интернет-отрасли, работающая с 1996 года. Направления деятельности РОЦИТ: популяризация, экспертиза и развитие интернета в России.

Фонд развития сети Интернет "Дружественный Интернет" учрежден Центром Анализа Интернет Ресурсов при активной поддержке ведущих участников интернет-индустрии. Главной целью Фонда является содействие развитию сети Интернет как благоприятной среды, дружественной ко всем пользователям.

Центр Безопасного Интернета (Национальный Узел Интернет-безопасности в России) - член Международной сети "горячих линий" по борьбе с противоправным контентом INHOPE – <http://www.detivrunete.ru/>

Задачи программы «Безопасный Интернет»: создание «горячей линии» в сети Интернет для выявления фактов распространения информации о нелегальной торговле детьми, детской порнографией, иной противозаконной или вредной для детей информации; оказание юридической помощи гражданам Российской Федерации по вопросам, связанным с борьбой с торговлей детьми и детской порнографией, а также с распространением иной противозаконной или вредной для детей информации в сети Интернет или сетях мобильной телефонной связи; проведение семинаров и конференций по проблемам, связанным с борьбой с торговлей детьми и детской порнографией, а также с распространением иной противозаконной или вредной для детей информации в сети Интернет или сетях мобильной телефонной связи; создание и поддержка информационных сайтов Программы в сети Интернет; сотрудничество с международными организациями, целями которых являются борьба с торговлей детьми и детской порнографией, противозаконной и вредной для детей информацией в сети Интернет и сетях мобильной телефонной связи.

По телефону **8-800-200-24-00** предоставляются психологические консультации по проблемам насилия и принуждения к сексуальной

эксплуатации, а также помочь жертвам подобных преступлений. Все консультации, а также звонок на телефонный номер Линии помощи, бесплатны; консультации предоставляются круглосуточно. Телефонная Линия помощи поддерживается партнерами Центра безопасного Интернета в России.

Можно получить удаленную консультацию с помощью сайта безопасного Интернета. Для этого на сайте Центра Безопасного Интернета предлагается с указанием Интернет-адреса сообщаемого ресурса сообщить о противоправном контенте в Интернете по следующим рубрикам:

- Сексуальная эксплуатация детей, детская порнография
- «Завлечение» педофилями детей в Интернете
- Расизм, национализм, ксенофобия, пропаганда сектантов
- Киберунижение, оскорблений и травля в Сети
- Пропаганда и публичное оправдание терроризма
- Пропаганда насилия и преступлений в Интернете
- Пропаганда наркотиков, их употребления
- Мошенничество в Интернете, информация о вредоносных программах
- Другие виды противоправного контента

Лига безопасного Интернета – крупнейшая и наиболее авторитетная в России организация, созданная при поддержке Минкомсвязи РФ в январе 2011 года для борьбы с опасным контентом во всемирной сети путем самоорганизации профессионального сообщества, участников интернет-рынка и рядовых пользователей.
<http://www.ligainternet.ru/>.

В Лигу безопасного интернета входят ведущие телекоммуникационные операторы, ИТ-компании, интернет-ресурсы и общественные организации.

Участниками Лиги являются все общественные организации, которые так или иначе заняты проблемой безопасного Интернета: Фонд развития Интернета, Фонд «Дружественный рунет», РОЦИТ со своим Центром безопасного Интернета в России. Большая часть разработчиков программных продуктов родительского контроля также присоединилась к Лиге». Попечительский совет лиги возглавляет министр связи и массовых коммуникаций Российской Федерации Игорь Щеголев. Учредитель Лиги безопасного интернета - Благотворительный фонд Святителя Василия Великого.

Лига занимается проблемами безопасности детей в сети. Среди них – масштабное распространение детской порнографии, всплеск сексуального насилия в отношении несовершеннолетних.

Линия помощи «Дети онлайн». Фонд «Дружественный Рунет», Фонд Развития Интернет, «КОМСТАР — Объединенные ТелеСистемы» (ОАО «КОМСТАР-ОТС», LSE: CMST), крупнейший оператор интегрированных телекоммуникационных услуг в России и СНГ, и «Московская городская телефонная сеть» (МГТС), входящая в Группу «КОМСТАР-ОТС», запустили в рамках Года Безопасного Интернета (2009 г.) всероссийский общественный проект – **интерактивная Линия помощи «Дети онлайн»**. Это служба телефонного и онлайн консультирования по проблемам безопасного использования сети Интернет и мобильной связи для детей, подростков, родителей и работников образовательных и воспитательных учреждений. Обратившись на Линию, пользователи могут получить квалифицированную помощь специалистов по вопросам безопасного пользования сетью Интернет и мобильной связью.

Линия помощи «Дети онлайн» начала работу в тестовом режиме 15 декабря 2009 года. В рамках реализации проекта «КОМСТАР-ОТС» как оператор дальней связи выделил единый федеральный номер **8-800-25-000-15** с возможностью совершения бесплатных междугородных звонков по всей территории России (услуга «Бесплатный вызов»), а МГТС предоставила рабочие места для операторов Линии в call-центре крупнейшей в стране справочно-сервисной службы 009.

На Линии помощи «Дети онлайн» работают профессиональные эксперты – психологи Фонда Развития Интернет и факультета психологии МГУ имени М.В. Ломоносова. В режиме телефонного и онлайн консультирования специалисты оказывают профессиональную психологическую и информационную помощь детям, подросткам, родителям и педагогам по безопасному использованию интернета и мобильной связи детьми.

Целевая аудитория: несовершеннолетние (до 18 лет) пользователи Интернета и мобильной связи; родители; работники образовательных и воспитательных учреждений (преподаватели, учителя, классные руководители, воспитатели).

Задачи проекта: психологическая помощь детям и подросткам, столкнувшимся с опасностью во время пользования Интернетом и/или мобильной связью; информационная и консультационная поддержка детей, подростков, родителей и работников образовательных и воспитательных учреждений по проблемам безопасного использования сети Интернет и мобильной связи детьми.

Обратиться на Линию помощи можно, позвонив на бесплатный федеральный номер 8-800-25-000-15 (с 9 до 18 часов по московскому времени в рабочие дни) или отправив письмо по электронной почте: helpline@detionline.org. Сайты Линии помощи: www.detionline.com, www.detionline.org.

Корпорация Microsoft поддерживает усилия Евросоюза и входящих в него стран-участников по совершенствованию мер безопасности детей в Интернете и занимается разработкой высокотехнологичных методов решения проблем безопасности и защищенности в работе с компьютером.

Microsoft на своих вебсайтах информирует общественность – особенно родителей и учителей – о мерах, помогающих обезопасить интерактивное пребывание детей в Интернете. Например, сетевой сервис MSN 8 корпорации Microsoft включает в себя «средства родительского контроля», позволяющие родителям ограничивать своих детей в использовании Интернета и общении через него.

Microsoft поддерживает паневропейскую организацию IN-HOPE, расширяющую и укрепляющую связи между европейскими «горячими линиями» Интернета, созданными смарт-процессором SIAP. Microsoft также продолжает осуществлять сотрудничество с Интерполом и Международным центром защиты детей от эксплуатации и похищений (ICMEC), предоставляя международную программу подготовки сотрудников правоохранительных органов во всем мире, которые расследуют преступления против детей, совершаемые с помощью компьютера.

Microsoft считает, что программные рейтинговые услуги являются полезным средством повышения онлайновой детской безопасности. Например, проект INCORE (Определение рейтинга европейского Интернет-контента) был совместной инициативой государственного и частного секторов, реализованной Европейской Комиссией и рекомендовавшей использование рейтинговой системы фильтрации содержания (<http://www.staysafeonline.com/>).

2.6. Полезные ссылки

- **Европейская комиссия, Программа «Сейфер Интернет Плюс»:**
http://europa.eu.int/information_society/programmes/iap/index_en.htm
- **Рамочное решение Совета от 22 декабря 2003 г. о борьбе сексуальной эксплуатацией детей и детской порнографией:**
http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/L013/1_01320040120en00440048.pdf

Методические рекомендации «Основы медиабезопасности»

- Рекомендации Совета от 24 сентября 1998 г. о защите малолетних и человеческого достоинства:
http://europa.eu.int/eur-lex/pri/en/oj/dat/1998/1_270/L27019981007en00480055.pdf
- Решение Совета от 29 мая 2000 г. о борьбе с детской порнографией в Интернете:
<http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/M 38/M 3820000609en00010004.pdf>
- Рейтинг европейского Интернет-контента:
<http://www.icra.org/>
- Федерация интерактивного программного обеспечения Европы:
<http://www.eupolitix.com/EN/Forums/Interactive+Software+Federation+of+Europe/home.htm>
- Паневропейская игровая информация:
<http://www.pegi.info/>
- Международный центр защиты детей от эксплуатации и похищений:
<http://www.icmec.org/>
- Как защититься от интернет-угроз. Памятка для школьников, учителей, родителей.
http://rfdeti.ru/catalog/main_news/admin/upload/1270470934_memorandum.pdf

3. Ссылки на видеовыступления П.А.Астахова по медиабезопасности детей.

<http://www.rfdeti.ru/videos/0>



Уполномоченный при Президенте Российской Федерации по правам ребенка Павел Астахов провел первый урок Медиабезопасности в школе-интернате для детей-сирот и детей, оставшихся без попечения родителей, № 15 циркового профиля имени Ю.В. Никулина.



Павел Астахов: Взрослые должны учить ребенка правильно пользоваться интернетом

4. Рекомендации для проведения занятий с детьми и родительских собраний по медиабезопасности с учетом возрастных особенностей

Общим подходом к проведению занятий по медиабезопасности является комплексность, т.е. проведение взаимосвязанных по содержанию занятий с детьми и родительских собраний. Правила медиабезопасности обсуждаются и принимаются в детском сообществе совместно с родителями и педагогами, при этом и родительская общественность организует обсуждение обязательств и прав родителей по поддержке правил медиабезопасности детей. В организациях среднего профессионального образования, дополнительного образования детей, в организациях для детей-сирот и детей, оставшихся без попечения родителей, мероприятия по основам информационной безопасности детей («основы медиабезопасности») проводятся без родителей, роль «взрослой» стороны в переговорах о правилах информационной безопасности должны выполнить воспитатели, педагоги образовательных учреждений, приглашенные специалисты-эксперты в этой области.

4.1. В учреждениях дошкольного образования рекомендуется вначале провести родительские собрания по основным правилам информационной безопасности детей («основы медиабезопасности»). Суть мероприятия – обсуждение и принятие сообществом родителей группы, детского садика, «Правил медиабезопасности детей». За основу рекомендуется использовать Советы по безопасному использованию Интернета, разработанные корпорацией Майкрософт при помощи Американской академии педиатров (AAP). На собрании последовательно представляются советы корпорации Майкрософт, и организуется подробное обсуждение целесообразности этих правил. Педагог может использовать информацию из рекомендаций, подготовленных специалистами отдела по обеспечению деятельности Уполномоченного при Президенте Российской Федерации по правам ребенка (глава 2 Материалов). Правила медиабезопасности, о которых родители договорились на собрании, рекомендуется откопировать для всех родителей, в том числе и для тех, кто не смог принять участие в собрании, ярко и интересно представить в пространстве групп, и рассказать детям доступно по содержанию, в игровой форме.

Методические рекомендации «Основы медиабезопасности»

Советы корпорации Майкрософт по безопасности при использовании Интернета вместе с ребенком в возрасте от 2 до 10 лет	Правила безопасности пользования Интернетом для детей дошкольного возраста
1. Никогда не рано начинать формировать открытое и позитивное общение с детьми. Желательно поговорить с ними о компьютерах, ответить на их вопросы и удовлетворить любопытство.	1. Обсуждайте с родителями возможности компьютеров
2. Всегда сидите за компьютером вместе с детьми данного возраста, когда они подключаются к Интернету.	2. Путешествуйте по Интернету с родителями
3. Установите четкие правила по использованию Интернета.	3. Правила по использованию Интернета выполняйте без обмана
4. Наставляйте на том, чтобы дети не разглашали своей личной информации, например свое реальное имя, адрес, номер телефона или пароли, людям, которых они встречают в Интернете.	4. Не разглашайте в Интернете свою личную информацию (реальное имя, адрес, номер телефона, пароли)
5. Если на сайте детей просят указать свое имя, чтобы персонифицировать веб-материалы, помогите детям придумать псевдоним для работы в Интернете, который бы не выдавал никакой личной информации.	5. Придумайте для работы в Интернете вымышленное имя (псевдоним), которое не выдаст личной информации
6. Используйте средства семейной безопасности для создания соответствующих профилей для каждого члена семьи, а также для обеспечения фильтрации интернет-содержимого. Для получения дополнительной информации см. Функции семейной безопасности Windows Live, средства родительского контроля Windows 7 и Windows Vista. Защитите ваших детей от всплывающих окон с оскорбительным содержимым с помощью функции блокировки всплывающих окон, встроенных в браузер Internet Explorer..	6. С помощью взрослых своей семьи защитите себя от оскорбительной информации с помощью блокировки всплывающих окон
7. Все члены семьи должны показывать пример детям, которые	7. Берите пример с тех, кто ведет себя безопасно в Интернете

Методические рекомендации «Основы медиабезопасности»

только начинают пользоваться Интернетом.	
--	--

4.2. Для учащихся 2 – 4 классов – занятия можно провести в формате марафона «Медиабезопасность». Если в параллелях по три – пять классов, то можно провести марафон параллельно. Суть мероприятия – принятие сообществом учеников и родителей «Правил медиабезопасности». В качестве почетных гостей Марафона рекомендуется пригласить родителей учеников и старшеклассников (старших братьев, сестер). За основу рекомендуется использовать Советы по безопасному использованию Интернета, разработанные корпорацией Майкрософт при помощи Американской академии педиатров (AAP). Класс или группа учеников должны представить одно правило, выведенное из советов корпорации Майкрософт. Правила, о которых договорились на Марафоне полезно поместить в классных уголках, откопировать для домашних уголков учащихся. По итогам Марафона рекомендуется провести родительские собрания, на которых представить родителям Правила и принять решение родительского собрания о поддержке принятых учащимися Правил медиабезопасности.

**Советы корпорации Майкрософт по
безопасности при использовании
Интернета вместе с ребенком в возрасте от
2 до 10 лет**

Никогда не рано начинать формировать открытое и позитивное общение с детьми. Желательно поговорить с ними о компьютерах, ответить на их вопросы и удовлетворить любопытство.

Всегда сидите за компьютером вместе с детьми данного возраста, когда они подключаются к Интернету.

Установите четкие правила по использованию Интернета.

Наставайте на том, чтобы дети не

Правила медиабезопасности

Обсуждайте с родителями и учителями возможности компьютеров, задавайте вопросы – на них ответят с интересом

Путешествуйте по Интернету со старшими родственниками, учителями

Установите четкие правила по использованию Интернета, выполняйте их без обмана

Не разглашайте в Интернете

Методические рекомендации для организации мероприятий по основам информационной безопасности детей («основы медиабезопасности»)

разглашали своей личной информации, например свое реальное имя, адрес, номер телефона или пароли, людям, которых они встречают в Интернете.

Если на сайте детей просят указать свое имя, чтобы персонифицировать веб-материалы, помогите детям придумать псевдоним для работы в Интернете, который бы не выдавал никакой личной информации.

Используйте средства семейной безопасности для создания соответствующих профилей для каждого члена семьи, а также для обеспечения фильтрации интернет-содержимого. Для получения дополнительной информации см. Функции семейной безопасности Windows Live, средства родительского контроля Windows 7 и Windows Vista. Защитите ваших детей от всплывающих окон с оскорбительным содержимым с помощью функции блокировки всплывающих окон, встроенных в браузер Internet Explorer..

Все члены семьи должны показывать пример детям, которые только начинают пользоваться Интернетом.

свою личную информацию (реальное имя, адрес, номер телефона, пароли)

Придумайте для работы в Интернете вымышленное имя (псевдоним), которое не выдаст личной информации

С помощью взрослых своей семьи защитите себя от оскорбительной информации с помощью блокировки всплывающих окон

Берите пример с тех, кто ведет себя безопасно в Интернете

Ситуации для «проверки» знания правил медиабезопасности:

- Вы всегда мечтали иметь программу «Фотошоп». Наконец-то вы нашли её в Интернете и скачали. Активируя программу в компьютере, уже перед завершением процесса, вы прочитали следующее сообщение: «Для получения бесплатного сообщения с кодом введите номер вашего мобильного телефона». Как вы поступите?
- Находясь в Интернете, вы открыли очень важную для вас страничку. Но компьютер тут же отреагировал: «Этот файл угрожает безопасности вашего компьютера, содержит троянскую программу». Каковы ваши дальнейшие действия?

Методические рекомендации для организации мероприятий по основам информационной безопасности детей («основы медиабезопасности»)

- На сайте «Одноклассники» вы познакомились с интересным человеком. Через некоторое время «новый друг» просит встречи с вами на «нейтральной территории». Опишите ваши действия.
- Для скачивания файла в Интернете потребовали введения ваших личных данных. Как вы поступите?

При проведении урока в начальных классах рекомендуется использовать материалы, размещённые:

- на сайте интерактивного курса по Интернет-безопасности (<http://www.microsoft.com/eesti/education/veebivend/koomiksid/tus/html/etusivu.htm>) в разделе «Для учащихся» рассказы для детей 7-10 лет, а также в разделе «Тесты» (можно организовать on-line тестирование школьников 7-10 лет);
- на сайте (<http://www.onlandia.org.ua/ru-RU/>) On-ляндия. Безопасная веб-страница в разделе «Для детей 7-10 лет» рассказы в картинках, задания и вопросы;
- на сайте (<http://content-filtering.ru/aboutus/>) Информационно-аналитический ресурс «Ваш личный Интернет» в разделе «Юным пользователям» - «Дошкольники и младшие классы» подсказки и советы по безопасному поведению в сети Интернет;
- на сайте <http://stopfraud.megafon.ru/> федерального проекта по борьбе с мобильным мошенничеством компании МегаФон в разделах «Виды мошенничества» и «Наши рекомендации», а также советы родителям;
- на портале «Безопасный интернет» (<http://www.saferinternet.ru/>) законодательство в сфере информационной безопасности и другие разделы, содержащие материалы по теме «Безопасный интернет».
- В качестве видео заставки для классного часа или урока можно использовать <http://youtu.be/789j0eDgIZQ> мультфильм «Безопасный интернет», который разработала студия Mozga.ru, принимавшая участие в конкурсе "Безопасный интернет - детям!", проведенном Mail.ru, где заняла первое место.

4.3. Занятия с учащимися 5 – 7 классов предлагается провести в формате классных часов, на которых ученики представляют свои сообщения по советам корпорации Microsoft по безопасности при использовании Интернета для детей 11 – 14 лет. Смыслом выступлений подростков является аргументация ответов на вопросы и целях каждого конкретного совета корпорации Microsoft, предложенного родителям и учителям. В качестве экспертов рекомендуется пригласить родителей учеников и старших братьев, сестер, старшеклассников. Эксперты оценивают качество аргументации. Лучшие выступления рекомендуется отметить призами, дипломами экспертов.

Темы выступлений лучше выразить в вопросной, проблемной форме. Например:

Методические рекомендации для организации мероприятий по основам информационной безопасности детей («основы медиабезопасности»)

- В этом возрасте дети хорошо разбираются во всех вопросах, связанных с Интернетом, тогда зачем рекомендуется следить и контролировать их?
- Зачем рекомендуется использование средств интернет-безопасности, которые ограничивают доступ к содержимому и сайтам, а также предоставляют информацию о действиях в Интернете?
- С какой целью взрослые должны проследить за тем, чтобы дети в этом возрасте понимали, какую личную информацию не следует разглашать в Интернете?
- Постоянно находиться рядом с детьми в этом возрасте, чтобы контролировать их использование Интернета, практически нецелесообразно. Зачем Майкрософт советует компьютеры, подключенные к Интернету, устанавливать в открытом месте?

Советы корпорации Майкрософт по безопасности при использовании Интернета вместе с ребенком в возрасте от 11 до 14 лет

1. Важно формировать открытое и позитивное общение родителей, учителей и детьми. Поговорите о компьютерах, обсудите вопросы
2. Установите четкие правила по использованию Интернета.
3. Настаивайте на том, чтобы дети не разглашали своей личной информации, например свое реальное имя, адрес, номер телефона или пароли, людям, которых они встречают в Интернете.
4. Если на сайте детей просят указать свое имя, чтобы персонифицировать веб-материалы, помогите детям придумать псевдоним для работы в Интернете, который бы не выдавал никакой личной информации.
5. Используйте средства семейной безопасности для создания соответствующих профилей для каждого члена семьи, а также для обеспечения фильтрации интернет-содержимого.
6. Настройте средний уровень в средстве семейной безопасности, который накладывает некоторые ограничения на содержимое, сайты и действия в Интернете.
7. Компьютеры, подключенные к Интернету, следует устанавливать в

Методические рекомендации для организации мероприятий по основам информационной безопасности детей («основы медиабезопасности»)

открытом месте, где можно легко контролировать действия детей.

8. Защитите ваших детей от всплывающих окон с оскорбительным содержимым с помощью функции блокировки всплывающих окон, встроенных в браузер. Internet Explorer..
9. Попросите детей рассказать, не ощущали ли они неудобство или страх от уведенного в Интернете или в ходе общения с другими людьми. Проявляйте спокойствие и напомните детям, что их никогда не накажут за то, что они вам расскажут. Похвалите их и попросите их сообщить вам, если то же самое повторится еще раз.

По итогам классных часов рекомендуется провести классные родительские собрания, на которых представить родителям советы корпорации Майкрософт, рассказать об аргументах учащихся и принять решение родительского собрания о поддержке советов в семьях учащихся.

При проведении урока в **5 - 7 классах** рекомендуется использовать материалы, размещённые:

- на сайте интерактивного курса по Интернет-безопасности (<http://www.microsoft.com/eesti/education/veebivend/koomiksid/rus/ml/etusivu.htm>) в разделе «Для учащихся» рассказы для детей 11-16 лет, а также в разделе «Тесты» (можно организовать on-line тестирование школьников 11-14 лет);
- на сайте (<http://www.onlandia.org.ua/ru-RU/>) On-ляндия. Безопасная веб-страна в разделе «Для детей 11-14 лет» рассказы в картинках, задания и вопросы; в разделе «Для учителей» опасности в сети и поведение в сети;
- на сайте (<http://content-filtering.ru/aboutus/>) Информационно-аналитический ресурс «Ваш личный Интернет» в разделе «Юным пользователям» - «Средние классы» подсказки и советы по безопасному поведению в сети Интернет, а также при использовании онлайн-игр и мобильного телефона;
- на сайте <http://stopfraud.megafon.ru/> федерального проекта по борьбе с мобильным мошенничеством компании МегаФон в разделах «Виды мошенничества» и «Наши рекомендации», а также советы родителям;
- на портале «Безопасный интернет» (<http://www.saferinternet.ru/>) законодательство в сфере информационной безопасности и другие разделы, содержащие материалы по теме «Безопасный интернет».

4.4. С учащимися 8 – 9 классов рекомендуется провести круглый стол по обсуждению советов корпорации Майкрософт. Смыслом обсуждения является напоминание правил использования Интернета, мотивация ответственного, безопасного поведения в Интернете и социальных сетях. Подростки старше 14 лет имеют практически неограниченный доступ к содержимому Интернета, сайтам или действиям. Они хорошо разбираются с тем, как использовать Интернет, однако все равно следует напоминать им о соответствующих правилах безопасности. Родители и учителя всегда должны быть готовы помочь своим детям-подросткам разобраться, какие сообщения являются непристойными, а также избегать опасных ситуаций. Рекомендуется напоминать детям-подросткам о том, какую личную информацию не следует предоставлять через Интернет.

Позиционерами круглого стола могут быть:

- Специалисты по медиабезопасности крупной или средней компании, телефонной компании;
- Представители родительской общественности;
- Учащиеся – старшеклассники или студенты вузов;
- Учащиеся-подростки, имеющие авторитет среди учащихся как активные пользователи социальных сетей, Интернета
- Учителя информатики
- Школьный психолог и т.д.

Предметом обсуждения могут стать советы по медиабезопасности, которые особенно трудно выполнять детям-подросткам. С целью определения проблемного поля, рекомендуем провести анкетирование подростков на предмет определения, какие советы по медиабезопасности, особенно трудно выполнять детям-подросткам

Советы по медиабезопасности корпорации Майкрософт старшим подросткам

1. Страйтесь по-прежнему поддерживать как можно более открытое общение внутри семьи и

Вопросы анкеты «Советы по медиабезопасности корпорации Майкрософт старшим подросткам»

1. Открыто общайтесь в семье, поддерживайте позитивное отношение к компьютерам.

Методические рекомендации для организации мероприятий по основам информационной безопасности детей («основы медиабезопасности»)

позитивное отношение к компьютерам. Обсуждайте с детьми их общение, друзей и действия в Интернете точно так же, как другие действия и друзей. Просите детей-подростков рассказывать вам, если что-то или кто-то в Интернете доставляет им чувство неудобства или страха. Если вы подросток и вам не нравится что-то или кто-то в Интернете, расскажите об этом.

2. Создайте список семейных правил использования Интернета дома. Укажите виды сайтов, которые можно посещать без ограничений, время подключения к Интернету, расскажите, какую информацию не следует разглашать в Интернете, а также предоставьте инструкции по общению с другими в Интернете, включая общение в социальных сетях.
3. Компьютеры, подключенные к Интернету, должны находиться в открытом месте, а не в спальне ребенка-подростка.
4. Защитите ваших детей от всплывающих окон с оскорбительным содержимым с помощью функции блокировки всплывающих окон, встроенных в браузер Internet Explorer..
5. Следите за тем, какие сайты посещает ваш ребенок-подросток и с кем он общается. Просите их пользоваться контролируемыми чатами, настаивайте на том, чтобы они использовали только общедоступные чаты.

Обсуждайте с родителями Ваше общение, друзей и действия в Интернете точно так же, как другие действия и друзей. Рассказывайте, если что-то или кто-то в Интернете доставляет им чувство неудобства или страха. Если вам не нравится что-то или кто-то в Интернете, расскажите об этом.

2. Договоритесь о семейных правилах использования Интернета дома, о видах сайтов, которые можно посещать без ограничений, о времени подключения к Интернету. Помните, какую информацию не следует разглашать в Интернете, как общаться с другими в Интернете, включая общение в социальных сетях.
3. Компьютеры, подключенные к Интернету, должны находиться в открытом месте, а не в детской спальне.
4. Защититесь от всплывающих окон с оскорбительным содержимым с помощью функции блокировки всплывающих окон, встроенных в браузер Internet Explorer..
5. Пользуйтесь контролируемыми чатами, посещайте безопасные сайты и социальные сети

Методические рекомендации для организации мероприятий по основам информационной безопасности детей («основы медиабезопасности»)

6. Настаивайте на том, чтобы они никогда не соглашались на встречу с друзьями, с которыми они познакомились в Сети.
7. Научите детей не загружать программы, музыку или файлы без вашего разрешения. Обмен файлами и использование текста, изображений или рисунков с веб-сайтов может привести к нарушению авторских прав и может быть незаконным.
8. Поговорите со своими детьми-подростками о содержимом в Интернете, предназначенном для взрослых, и порнографии, а также укажите им позитивные сайты, посвященные вопросам здоровья и сексуальности.
9. Помогите им защитить себя от спама. Проинструктируйте своих детей-подростков никогда не давать свой адрес электронной почты при общении в Интернете, не отвечать на нежелательные почтовые сообщения и пользоваться фильтром электронной почты.
10. Знайте, какие сайты ваши дети-подростки посещают чаще всего. Убедитесь, что ваши дети не посещают сайты, содержащие оскорбительные материалы, и не публикуют свою личную информацию. Следите за тем, какие фотографии публикуют ваши дети-подростки и их друзья.
11. Учите своих детей отзывчивости, этике и правильному поведению в Интернете. Они не должны
6. Никогда не соглашайтесь на встречу с друзьями, с которыми познакомились в Сети.
7. Не загружайте программы, музыку или файлы без разрешения родителей. Обмен файлами и использование текста, изображений или рисунков с веб-сайтов может привести к нарушению авторских прав и может быть незаконным.
8. Не пользуйтесь содержимым в Интернете, предназначенном для взрослых, и порнографией, найдите позитивные сайты, посвященные вопросам здоровья и сексуальности.
9. Защитите себя от спама. Никогда не давайте свой адрес электронной почты при общении в Интернете, не отвечайте на нежелательные почтовые сообщения и пользуйтесь фильтром электронной почты.
10. Не посещайте сайты, содержащие оскорбительные материалы, и не публикуйте свою личную информацию. Следите за тем, какие фотографии публикуете Вы и Ваши друзья.
11. Не используйте Интернет для распространения сплетен, клеветы

Методические рекомендации для организации мероприятий по основам информационной безопасности детей («основы медиабезопасности»)

- использовать Интернет для распространения сплетен, клеветы или запугивания других.
12. Проследите за тем, чтобы дети спрашивали у вас, прежде чем совершать финансовые операции в Интернете, включая заказ, покупку или продажу товаров.
13. Обсудите со своими детьми-подростками азартные игры в Интернете, а также потенциальные риски, связанные с ними. Напомните им о том, что азартные игры в Интернете являются незаконными.
12. Спрашивайте у родителей, прежде чем совершать финансовые операции в Интернете, включая заказ, покупку или продажу товаров.
13. Обсудите с родителями азартные игры в Интернете, потенциальные риски, связанные с незаконными действиями

По итогам классных часов рекомендуется провести классные родительские собрания, на которых представить родителям советы корпорации Майкрософт, рассказать о проблематике медиабезопасности, которая была представлена участниками круглого стола. Родителям будет полезно повторить правила и отрефлексировать их.

При проведении урока **в 8-9 классах** рекомендуется использовать материалы, размещённые:

- на сайте интерактивного курса по Интернет-безопасности (<http://www.microsoft.com/eesti/education/veebivend/koomiksid/tus/html/etusivu.htm>) в разделе «Для учащихся» рассказы для детей 11-16 лет, а также в разделе «Тесты» (можно организовать on-line тестирование школьников 11-14 лет);
- на сайте (<http://www.onlandia.org.ua/ru-RU/>) On-ляндия. Безопасная веб-страна в разделе «Для детей 11-14 лет» рассказы в картинках, задания и вопросы; в разделе «Для учителей» опасности в сети и поведение в сети;
- на сайте (<http://content-filtering.ru/aboutus/>) Информационно-аналитический ресурс «Ваш личный Интернет» в разделе «Юным пользователям» - «Средние классы» подсказки и советы по безопасному поведению в сети Интернет, а также при использовании онлайн-игр и мобильного телефона;
- на сайте <http://stopfraud.megafon.ru/> федерального проекта по борьбе с мобильным мошенничеством компании МегаФон в разделах «Виды мошенничества» и «Наши рекомендации», а также советы родителям;
- на портале «Безопасный интернет» (<http://www.saferinternet.ru/>) законодательство в сфере информационной безопасности и другие разделы, содержащие материалы по теме «Безопасный интернет».

4.5. Старшеклассникам рекомендуется предложить провести мероприятия по медиабезопасности в начальной и основной школе, самим принять участие в жюри конкурсов младших подростков, круглых столах старших подростков, оформить классные уголки и школьные стенды интересными материалами по проблеме медиабезопасности. Посоветуйте старшеклассникам использовать материалы, размещённые:

- на сайте интерактивного курса по Интернет-безопасности (<http://www.microsoft.com/eesti/education/veebivend/koomiksid/rus/ml/etusivu.htm>) в разделе «Для учащихся» рассказы для детей 11-16 лет, а также в разделе «Тесты» (можно организовать on-line тестирование школьников 11-14 лет);
- на сайте (<http://www.onlandia.org.ua/ru-RU/>) On-ляндия. Безопасная веб-страна в разделе «Для подростков» советы по безопасному общению и работе в режиме on-line; в разделе «Для учителей» опасности в сети и поведение в сети;
- на сайте (<http://content-filtering.ru/aboutus/>) Информационно-аналитический ресурс «Ваш личный Интернет» в разделе «Юным пользователям» - «Старшие классы» подсказки и советы по безопасному поведению в сети Интернет, а также при использовании онлайн-игр и мобильного телефона;
- на сайте <http://stopfraud.megafon.ru/> федерального проекта по борьбе с мобильным мошенничеством компании МегаФон в разделах «Виды мошенничества» и «Наши рекомендации», а также советы родителям;
- на портале «Безопасный интернет» (<http://www.saferinternet.ru/>) законодательство в сфере информационной безопасности и другие разделы, содержащие материалы по теме «Безопасный интернет».

5. Советы родителям: Как помочь вашим детям более безопасно пользоваться сайтами социальных сетей?

<http://www.microsoft.com/ru-ru/security/family-safety/kids-social.aspx>

Сегодня многие дети не делают различий между реальной жизнью и виртуальной жизнью в Интернете. Они могут пользоваться сайтами социальных сетей, предназначенных для детей, такими как Webkinz или Club Penguin, или сайтами социальных сетей, предназначенных для взрослых, такими как Windows Live Spaces,

Методические рекомендации для организации мероприятий по основам информационной безопасности детей («основы медиабезопасности»)

YouTube, MySpace, Flickr, Twitter, Facebook и другими. Что бы они ни делали, они должны понимать, что многие из этих веб-страниц могут просматривать кто угодно, кто обладает доступом в Интернет.

Дети могут использовать эти сайты для: чата; игр; публикации и просмотра фотографий и видео; блог, публикации профиля в Интернете.

К сожалению, часть информации, которые дети публикуют на своих страницах, может также делать их уязвимыми для **фишинговых сообщений**, киберугроз и интернет-похитителей. Далее описано несколько способов, как вы можете помочь детям более безопасно пользоваться сайтами социальных сетей.

- **Поговорите с детьми об опыте их общения в социальных сетях.** Попросите детей рассказывать вам, если они столкнутся на этих сайтах с чем-либо, что вызывает у них беспокойство, неудобство или страх. Проявляйте спокойствие и напомните детям, что их никогда не накажут за то, что они вам расскажут. Дайте детям понять, что вы вместе с ними постараетесь найти удачный выход из сложившейся ситуации.
- **Установите собственные правила пользования Интернетом у вас дома.** Как только дети начнут самостоятельно пользоваться Интернетом, желательно подготовить список правил пользования Интернетом, которые будут приняты всеми. В этих правилах должно быть указано, могут ли дети использовать сайты социальных сетей и каким образом. Для получения дополнительных сведений о том, как установить правила, см. [Использование семейных контрактов для защиты детей в Интернете](#).
- **Проследите за тем, чтобы дети соблюдали возрастные ограничения на сайте.** Рекомендуемый возраст для регистрации на сайтах социальных сетей обычно составляет 13 или более лет. Если ваши дети не достигли рекомендуемого возраста, указанного для данных сетей, не разрешайте им пользоваться сайтами. Важно помнить, что вы не должны полностью полагаться на службы сайта, которые не допускают регистрации детей, не достигших нужного возраста.
- **Научитесь пользоваться сайтом.** Оцените сайты, которые планирует использовать ваш ребенок, и убедитесь, что вы и ваш ребенок понимают политику конфиденциальности и правила поведения. Узнайте, существует ли на сайте контроль над публикуемым содержимым. Кроме того, периодически просматривайте страницу вашего ребенка. Для получения дополнительных предложений см. [Советы по безопасному ведению блогов для детей и родителей](#).

Методические рекомендации для организации мероприятий по основам информационной безопасности детей («основы медиабезопасности»)

- **Настаивайте на том, чтобы дети никогда лично не встречались с тем, с кем они общались только по Интернету, и просите их общаться только с теми, кого они знают лично.** Дети подвергаются реальной опасности во время личной встречи с незнакомыми людьми, с которыми они общались только по сети. Вы можете защитить своих детей, попросив их общаться в Интернете со своими друзьями и не общаться с теми, с кем они лично не встречались. Иногда бывает недостаточно просто сказать детям, чтобы они не разговаривали с незнакомыми людьми, поскольку дети могут не считать незнакомым человека, с которым они «встречались» в сети. Для получения дополнительных советов по защите ваших детей в Интернете см. [Интернет-преступники: что можно сделать, чтобы уменьшить риск](#).
- **Убедитесь в том, что ваши дети не указывают свои полные имена.** Проследите за тем, чтобы дети использовали только свои имена или псевдонимы, но никогда не использовали псевдонимы, которые бы вызывали ненужное внимание. Кроме того, не разрешайте своим детям публиковать полные имена своих друзей.
- **Опасайтесь наличия в профиле ребенка информации, по которой можно идентифицировать его личность.** На многих сайтах социальных сетей дети могут присоединяться к общественным группам, включающим учеников определенной школы. Будьте бдительны, если дети разглашают эту и другую информацию, которую можно использовать для их идентификации, например школьный питомец-талисман, рабочие места и название города проживания. Если указано слишком много информации, ваши дети могут подвергаться киберугрозам, атакам со стороны интернет-преступников, интернет-мошенников или краже личных данных. Для получения дополнительной информации см. [Распознавание фишинговых и поддельных сообщений электронной почты](#).
- **Постарайтесь выбрать сайт, который не столь широко используется.** Некоторые сайты позволяют защитить вашу страницу с помощью пароля или другими способами, чтобы ограничить круг посетителей, разрешив его только тем лицам, которых знает ваш ребенок. Например, с помощью Windows Live Spaces вы можете настроить разрешения, указав тех, кто может посещать ваш сайт. При этом возможны самые различные настройки – от всех пользователей Интернета до ограниченного списка людей.
- **Следите за деталями на фотографиях.** Объясните детям, что фотографии могут раскрывать много личной информации. Попросите детей не публиковать фотографии себя или своих друзей, на которых имеются четко

Методические рекомендации для организации мероприятий по основам информационной безопасности детей («основы медиабезопасности»)

идентифицируемые данные, такие как названия улиц, государственные номера автомобилей или название школы на одежде.

- **Предостерегите своего ребенка относительно выражения своих эмоций перед незнакомцами.** Вероятно, вы уже предупреждали своих детей не общаться с незнакомыми людьми напрямую по сети. Однако дети используют сайты социальных сетей для написания журналов и стихотворений, в которых часто выражают сильные чувства. Объясните детям, что многое из публикуемого сможет прочесть любой пользователь, имеющий доступ в Интернет, а также что похитители часто ищут эмоционально уязвимых детей. Для получения дополнительной информации см. [Чему следует научить детей, чтобы повысить их безопасность при работе в Интернете](#).
- **Расскажите детям об интернет-угрозах.** Как только ваши дети станут достаточно взрослыми для использования социальных сетей, поговорите с ними о киберугрозах. Расскажите детям, что если у них возникнет ощущение, что им угрожают через Интернет, то им сразу же следует сообщить об этом родителям, учителю или другому взрослому человеку, которому они доверяют. Кроме того, очень важно научить детей общаться по сети точно так же, как они общаются лично. Попросите детей относиться к другим людям так же, как они хотели бы, чтобы относились к ним самим.
- **Удаление страницы вашего ребенка.** Если ваши дети откажутся следовать установленным правилам, которые предназначены для их безопасности, и вы безуспешно пытались их убедить следовать им, то вы можете обратиться на сайт социальной сети, который использует ваш ребенок, и попросить удалить его страницу. Можно также обратить внимание на средства фильтрации интернет-содержимого (например, [Функции семейной безопасности Windows Live](#)) в качестве дополнения и ни в коем случае не замены для контроля со стороны родителей.

6.Обучение детей основам безопасности при работе с Интернетом

<http://www.microsoft.com/ru-ru/security/family-safety/kids-social.aspx>

Научите детей никому не сообщать пароли

Дети создают имена пользователей и пароли для доступа на сайт школы, игровые сайты, в социальные сети, для публикации фотографий, совершения покупок в Интернете и других операций. Согласно данным исследования [Teen Angels](#) из [Wired Safety.org](#), 75 процентов детей в возрасте от 8 до 9 лет сообщают свои пароли другим лицам, 66 процентов девочек в возрасте 7-12 признались, что сообщали свой пароль другим лицам. Первое правило

Методические рекомендации для организации мероприятий по основам информационной безопасности детей («основы медиабезопасности»)

безопасности при работе в Интернете: пароли следует держать в секрете. Научите детей хранить свои пароли столь же бережно, как информацию, которую они хотят защитить.

Далее приведены некоторые правила, которые дети должны знать и соблюдать.

- **Никогда не сообщайте свои пароли другим.** Не показывайте никому свои пароли, даже друзьям.
- **Обеспечьте защиту для записанных паролей.** Будьте внимательны к тому, где вы храните или записываете пароли. Не храните пароли в рюкзаке или бумажнике. Не оставляйте данные о паролях в местах, где вы бы не хотели оставить информацию, защищенную с их помощью. Не храните пароли в файле на компьютере. Преступники ищут там в первую очередь.
- **Никогда не предоставляйте свой пароль по электронной почте или в ответ на запрос по электронной почте.** Любое сообщение электронной почты, в котором вас просят указать пароль или перейти на веб-сайт, чтобы проверить пароль, может представлять собой разновидность мошенничества, которая называется фишингом. К ним относятся запросы с сайтов, вызывающих доверие, которые вы можете постоянно посещать. Мошенники часто создают поддельные сообщения электронной почты, содержащие такие же логотипы как и на реальных сайтах и написанных таким языком, чтобы не вызывать сомнения в своей достоверности. [**Дополнительные сведения о фишинговых сообщениях**](#).
- **Не вводите пароли на компьютерах, которые вы не контролируете.** Не пользуйтесь общедоступными компьютерами в школе, библиотеке, в интернет-кафе или в компьютерных лабораториях, кроме как для анонимного просмотра страниц в Интернете.

Не используйте эти компьютеры с учетными записями, где требуется вводить имя пользователя и пароль. Преступники могут за очень небольшие деньги приобрести устройства, регистрирующие нажатия клавиш, которые устанавливаются в течение нескольких секунд. С помощью подобных устройств злоумышленники могут собирать информацию, вводимую на компьютере, через Интернет.

Если ваши дети пишут блоги, убедитесь в том, что они не рассказывают слишком много о себе.

Практика написания блогов (сокращение от англ. "web log" – дневник в сети) или личного интерактивного журнала очень быстро стала популярной среди подростков, многие из которых ведут свои блоги без ведома родителей или опекунов. Социальные сети сейчас обошли по популярности блоги среди большинства подростков, однако многие дети по-

Методические рекомендации для организации мероприятий по основам информационной безопасности детей («основы медиабезопасности»)

прежнему ведут свой блог на своем сайте социальной сети. Недавние исследования показали, что на сегодняшний день примерно половину всех блогов пишут подростки, при этом каждые двое из троих указывают свой возраст, каждые трое из пяти сообщают о месте своего проживания и дают контактную информацию, а каждый пятый указывает свое полное имя. Разглашение подробной личной информации сопряжено с риском. Несмотря на то, что ведение блога дает возможные преимущества, включая развитие навыков письма и общения, очень важно рассказать детям об Интернете и научить их писать блоги еще до того, как они начнут этим заниматься аналогично тому, как все сначала оканчивают курсы по вождению, прежде чем самостоятельно садятся за руль автомобиля. Далее приведены некоторые начальные советы.

- **Определите правила пользования Интернетом с детьми и проявите настойчивость.**
- **Просматривайте то, что дети планируют опубликовать в Интернете, прежде чем они опубликуют эти материалы.** Внешне безобидную информацию, например школьное животное-талисман и фотография города, можно собрать воедино и понять, в какую школу ходит автор.
- **Спросите себя (и проинструктируйте детей делать то же самое), насколько комфортно вы будете чувствовать себя, показывая эти материалы незнакомцу.** Если имеются сомнения, исключите такие материалы.
- **Проведите оценку службы блогов** и выясните, обеспечивает ли она возможность написания личных блогов, защищенных с помощью паролей.
- **Сохраните интернет-адрес блога вашего ребенка** и регулярно проверяйте его.
- **Просматривайте другие блоги, отыскивая положительные примеры для подражания для ваших детей.**

Помните об интернет-мошенниках.

Согласно данным Федеральной торговой комиссии США, 31 процент жертв похищения личных данных составляют молодежь. Подростки становятся привлекательными объектами для мошенников, поскольку, по сравнению с взрослыми они меньше заботятся о безопасном хранении информации.

Некоторые моменты, о которых должны знать ваши дети, чтобы стать разумными потребителями и избежать интернет-мошенничества.

- **Никогда не разглашайте личную информацию.**

Методические рекомендации для организации мероприятий по основам информационной безопасности детей («основы медиабезопасности»)

Никогда не указывайте свою личную информацию, например полное имя или город проживания во время общения с помощью мгновенных сообщений или в чатах, если вы полностью не уверены в личности человека, с которым вы общаетесь.

- **Обязательно завершайте сеанс с выходом из системы при работе на общедоступном компьютере.**

Если вы используете компьютер в библиотеке или в интернет-кафе, прежде чем покинуть компьютер, полностью завершите все сеансы с выходом из системы. Вы не знаете, какое программное обеспечение установлено на этих компьютерах, а также что оно выполняет. Кроме того, может быть установлено программное обеспечение, фиксирующее нажатие клавиш.

- **Придумывайте безопасные пароли и держите их в секрете.**

Для получения дополнительных сведений см. пункт 1 выше.

- **Используйте только безопасные сайты.**

Если ваши дети совершают покупки в Интернете, то им следует каждый раз убеждаться в том, что URL-адрес сайта, на котором они вводят финансовую информацию, начинается с префикса `https://`, в правом нижнем углу имеется желтый значок замка или адресная строка отображается зеленым цветом. Они могут щелкнуть по значку замка или в адресной строке, чтобы проверить сертификат безопасности данного сайта.

- **Распознавание мошенников и сообщение о фактах мошенничества.**

Расскажите своим детям о признаках подделки идентификационных данных: предложение утвержденных кредитных карт, звонки из агентств по сбору информации или незнакомые финансовые документы. Если у вашего ребенка возникнет подозрение на подделку личных данных, немедленно предпримите соответствующие действия, чтобы ограничить ущерб. Обратитесь в свою кредитную компанию, банки или все три организации по кредитной отчетности, а также в полицию. Закройте все счета, которые подвергались фальсификации, и попросите детей поменять пароли для всех своих учетных записей в Интернете. Ведите журнал всех выполняемых действий.

7.Советы по медиабезопасности от сотовой компании «Мегафон»

При использовании коротких premium номеров SMS

- Уточняйте у Оператора (на сайте, в Абонентской службе) и на специализированных ресурсах стоимость отправки SMS

Методические рекомендации для организации мероприятий по основам информационной безопасности детей («основы медиабезопасности»)

- При скачивании контента на Интернет-ресурсах внимательно читайте Условия использования сервиса, а также информацию, размещенную с символом «звездочка» (*)

При работе в сети интернет

- Устанавливайте на компьютер хорошо зарекомендовавшие себя антивирусные программы и межсетевые экраны (Firewall) и своевременно их обновляйте
- При скачивании контента внимательно читайте Условия использования сервиса, а также информацию, размещенную с символом «звездочка» (*)
- Не устанавливайте сомнительное программное обеспечение на свой компьютер / мобильный телефон.
- Не открывайте и не запускайте (*.exe) вложенные файлы неизвестного происхождения
- Будьте осторожны при всплывающих окнах, не переходите по неизвестным ссылкам
- Не отправляйте SMS для разблокировки Windows и разархивирования файлов

При заражении компьютера вирусом-вымогателем Trojan.Winlock

- Не обращайте внимания на требование вымогателей перечислить деньги
- Зайдите на специальный ресурс Dr.Web и получите БЕСПЛАТНО коды Разблокировки
- Скачайте бесплатную утилиту Dr.Web CureIt! и избавьте свой компьютер от вредоносных объектов
- Если действия вредоносных программ сделали невозможной загрузку Вашего компьютера, скачайте бесплатно Dr.Web LiveCD! и восстановите его работоспособность
- В случае возникновения дополнительных вопросов обращайтесь на официальный форум компании «Доктор Веб» в раздел «Помощь по лечению»

Используйте наши новые услуги

- Услуга «Мобильный прайс»
- Услуга «Блокировка отправки SMS на короткие номера»

При попытках явного и скрытого вымогательства

- Избегайте или сводите к минимуму передачу любой конфиденциальной информации (номера кредитных карточек, PIN-коды, пароли и т.д.).

Методические рекомендации для организации мероприятий по основам информационной безопасности детей («основы медиабезопасности»)

- Не переводите денежные средства на номера, указанные в SMS от неизвестных или сомнительных отправителей
- При просьбах вернуть ошибочно зачисленные на Ваш лицевой счет средства предлагайте обращаться к Оператору
- Перезванивайте человеку, с которым якобы случилось несчастье, или тем, кто в настоящий момент может находиться рядом с ним, если вдруг номер вашего родственника

При использовании голосовых premium номеров

- При неотвеченных звонках не перезванивайте на незнакомые номера (особенно международные)
- Уточняйте у Оператора (на сайте, в Абонентской службе) и на специализированных ресурсах стоимость минуты разговора
- При получении информации о выигрыше приза не звоните сразу же на указанный в сообщении короткий номер, уточните информации о проведении розыгрыша у организатора акции (на сайте, при звонке на городской номер)

При желании помочь обратившемуся на улице человеку

- Не отдавайте телефон в руки незнакомцев, предложите самостоятельно набрать нужный номер и передать информацию.

При получении сообщения о задолженности по номеру, который вы не подключали

- Обратитесь в офис обслуживания Оператора для оформления заявления о непричастности к Договору.