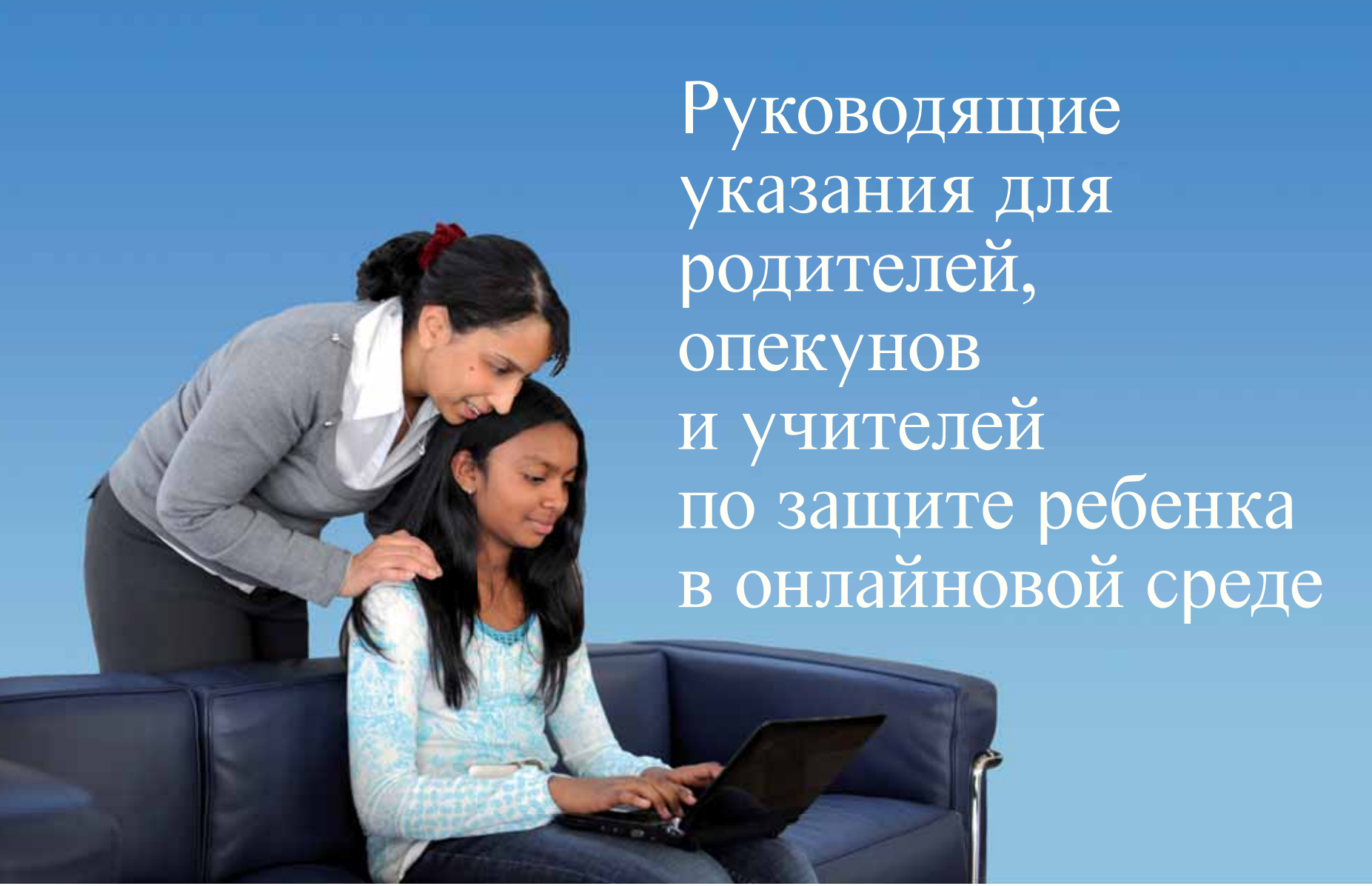


Руководящие указания для родителей, опекунов и учителей по защите ребенка в онлайновой среде

www.itu.int/cop

БЛАГОДАРНОСТИ

Данные Руководящие указания подготовлены МСЭ и командой авторов из ведущих организаций, работающих в отрасли ИКТ, и они не смогли бы состояться без затраченного ими времени, присущего им энтузиазма и самоотверженности.
МСЭ благодарит всех следующих авторов, потративших свое драгоценное время и знания (перечислены в алфавитном порядке):

- Кристна Буети (Cristina Bueti) и Сандра Панди (Sandra Pandi) – МСЭ
- Джонн Карр (John Carr) – Детская благотворительная коалиция за безопасность интернета
- Этель Куэйль (Ethel Quayle) – Эдинбургский университет, Соединенное Королевство
- Жанис Ричардсон – В безопасной сети
- Изабелла Санта (Isabella Santa) – Европейское Агентство по безопасности сетей и информации
- Маргарета Трунг (Margareta Traung) – Программа Европейской Комиссии за безопасный интернет
- Невин Тевфик (Nevine Tewfik) – Инициатива КиберМир, разработанной Международным женским движением за мир Сюзанны Мубарак

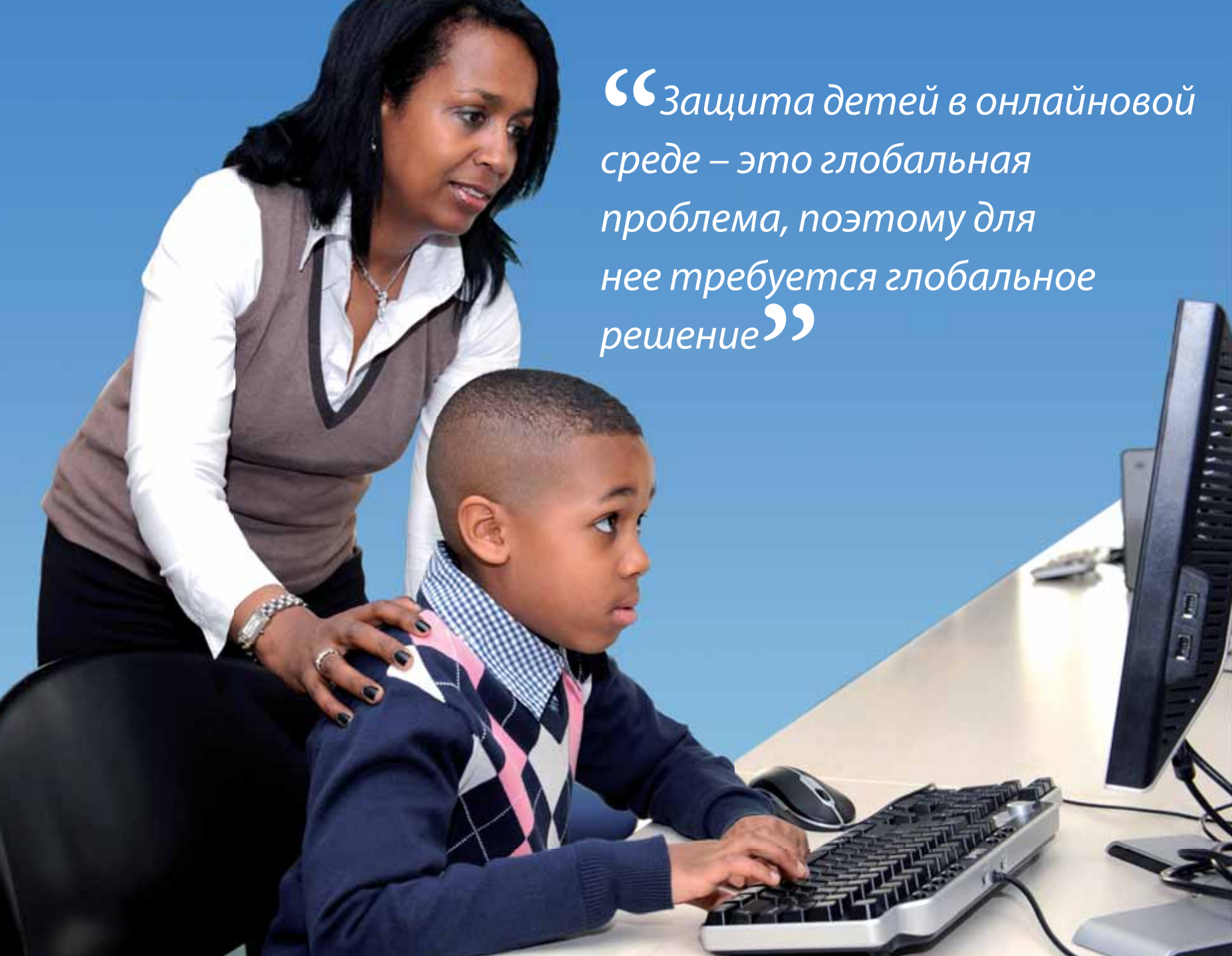
Авторы хотели бы поблагодарить Джонна Карра (John Carr) из CHIS, Соню Биллард и Кристину Агбтон-Джонсон из UNIDIR и Катерину Кристаки из ENISA за их подробный разбор и комментарии.

МСЭ хотел бы поблагодарить Сальму Аббаси из eWWG за ее неоценимое участие в инициативе "Защита ребенка в онлайновом режиме" (COP).

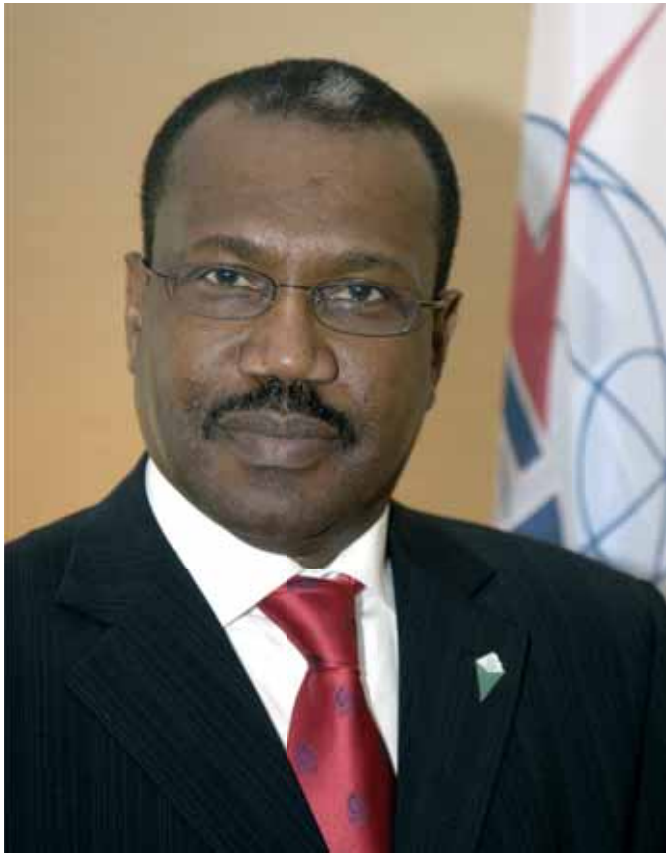
Дополнительная информация по этому проекту Руководящих указаний размещена по адресу: http://www.itu.int/cop/, и будет регулярно обновляться.

Если у вас есть какие-либо замечания, или вы хотели бы предоставить дополнительную информацию, пожалуйста, свяжитесь с г-жой Карлой Личчиарделло (Ms. Carla Licciardello) по адресу: cop@itu.int.

Содержание


“Защита детей в онлайновой среде – это глобальная проблема, поэтому для нее требуется глобальное решение”

Предисловие



Я с радостью пользуюсь этой возможностью рассмотреть вместе с вами предварительный вариант руководящих указаний, которые разработаны при неоценимой помощи многочисленных участников.

Защита ребенка в онлайновой среде в эру общедоступного широкополосного интернета является важнейшей проблемой, которая срочно требует глобальной скоординированной реакции. Хотя местные и даже национальные инициативы прочно заняли свое место, интернет не знает границ и международное сотрудничество могло бы стать ключом к нашему успеху и победе на поле предстоящей битвы.

Родители, опекуны и учителя – ключевые участники, которые помогут одержать победу в борьбе против киберпреступлений и киберугроз, и я лично очень благодарен вам за вашу поддержку.

Д-р Хамадун И. Туре
Генеральный секретарь Международного союза электросвязи (МСЭ)

Резюме

Интернет принес несказанные преимущества всем детям мира, и из года в год растет количество домохозяйств с выходом в интернет. К началу 2009 года интернетом пользовалось более 1,5 миллиардов человек, по сравнению с менее 200 миллионов в начале 1998 года.

Но хотя потенциальные блага бесспорны, интернет также принес с собой и некоторые новые проблемы, внушающие беспокойство, особенно если затронуты дети.

Современные молодые люди очень хорошо знакомы с техникой. Они также могут быстро написать сложные программы и приложения как на компьютере, так и на мобильном телефоне или других персональных устройствах, и похоже они делают это почти интуитивно. С другой стороны, когда дело касается компьютерных программ, мобильных телефонов или персональных устройств, взрослым, как правило, требуется инструкция пользователя для решения задач, о которых большая часть детей сказала бы, что это совсем простая задача. Однако взрослые могут привнести в обсуждения электронной безопасности свои неоценимые навыки и жизненный опыт.

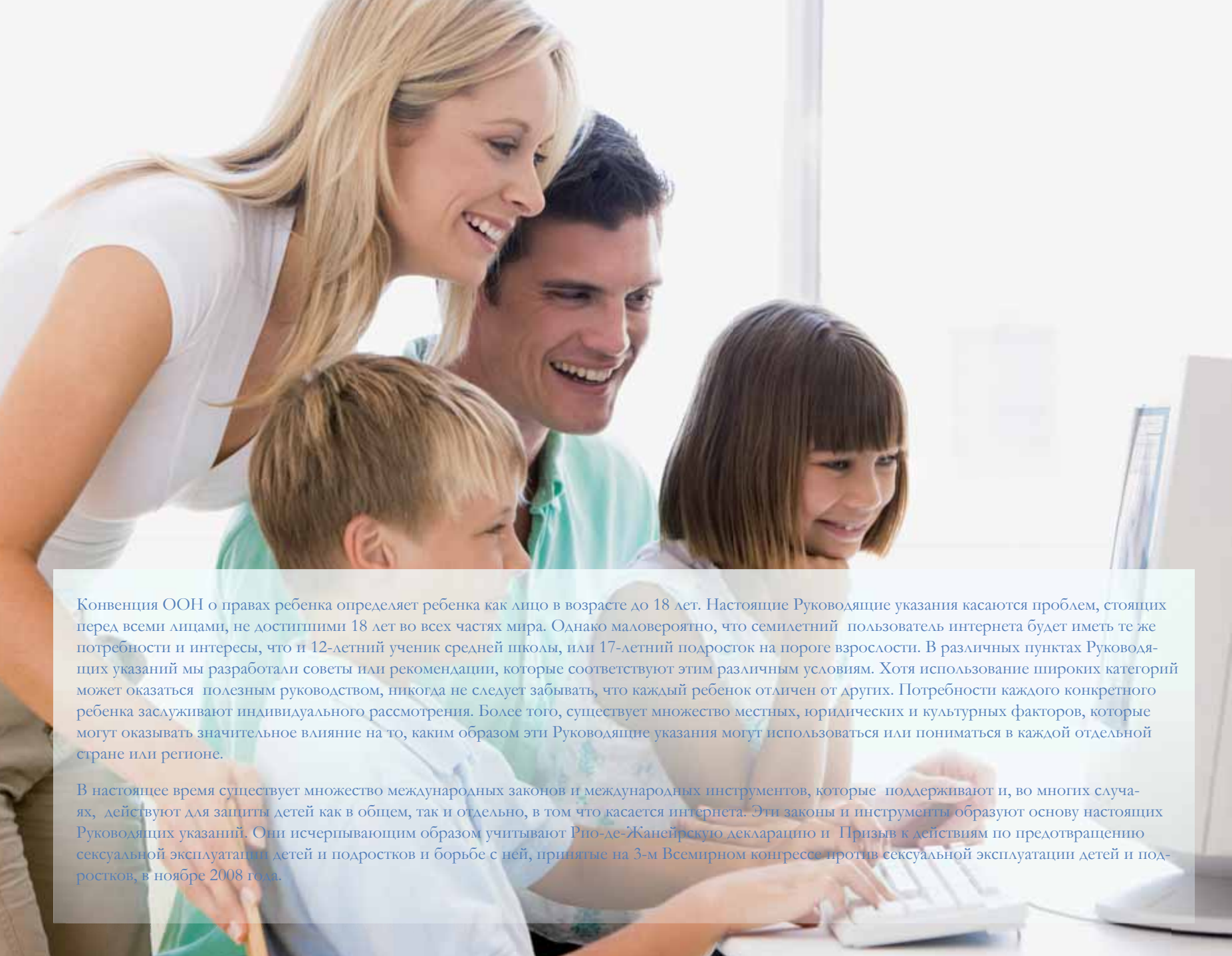
Очень важно определить, что дети и молодые люди действительно делают в онлайновой среде, а не то, что взрослые думают о том, что они делают. Исследования показывают, что все чаще дети соединяются с интернетом, используя игровые консоли и мобильные устройства, в то время как многие взрослые даже не знают, что можно установить соединение, используя эти устройства.

Одной из ключевых проблем является то, что дети и молодые люди стремятся выходить в интернет в тех местах, о которых взрослые сказали им, что они безопасны, например, дома или в школе. Многие родители и опекуны придерживаются общепринятого ложного представления, что их дети находятся в большей безопасности, если они используют компьютер дома, чем когда они выходят в интернет вне дома. Это опасное заблуждение, потому что интернет может перенести детей и молодых людей практически в любое место мира, и в это время они могут подвергаться потенциально опасным рискам. Почти таким же, как если бы они находились в реальном мире.

Настоящие Руководящие указания разработаны в рамках инициативы "Защита ребенка в онлайновой среде" (COP)[1], как пункта Глобального плана действий МСЭ по кибербезопасности[2], с целью

[1] http://www.itu.int/cop

[2] http://www.itu.int/osg/csd/cybersecurity/gca/



Конвенция ООН о правах ребенка определяет ребенка как лицо в возрасте до 18 лет. Настоящие Руководящие указания касаются проблем, стоящих перед всеми лицами, не достигшими 18 лет во всех частях мира. Однако маловероятно, что семилетний пользователь интернета будет иметь те же потребности и интересы, что и 12-летний ученик средней школы, или 17-летний подросток на пороге взрослости. В различных пунктах Руководящих указаний мы разработали советы или рекомендации, которые соответствуют этим различным условиям. Хотя использование широких категорий может оказаться полезным руководством, никогда не следует забывать, что каждый ребенок отличен от других. Потребности каждого конкретного ребенка заслуживают индивидуального рассмотрения. Более того, существует множество местных, юридических и культурных факторов, которые могут оказывать значительное влияние на то, каким образом эти Руководящие указания могут использоваться или пониматься в каждой отдельной стране или регионе.

В настоящее время существует множество международных законов и международных инструментов, которые поддерживают и, во многих случаях, действуют для защиты детей как в общем, так и отдельно, в том что касается интернета. Эти законы и инструменты образуют основу настоящих Руководящих указаний. Они исчерпывающим образом учитывают Рио-де-Жанейрскую декларацию и Призыв к действиям по предотвращению сексуальной эксплуатации детей и подростков и борьбе с ней, принятые на 3-м Всемирном конгрессе против сексуальной эксплуатации детей и подростков, в ноябре 2008 года.

создания основ для защищенного и безопасного кибермира, не только для сегодняшней молодежи, но также и для будущих поколений.

Предполагается, что Руководящие указания будут действовать как концептуальный проект, который может быть одобрен и может использоваться таким образом, который соответствует национальным местным традициям и законам. Более того, было бы желательно, чтобы эти руководящие указания рассматривали проблемы, которые могут затронуть всех детей и молодых людей младше 18 лет, но у каждой возрастной группы – свои потребности, заслуживающие отдельного рассмотрения.

Эти Руководящие указания подготовлены МСЭ в обстановке тесного сотрудничества команды самоотверженных авторов из ведущих организаций, действующих в отрасли ИКТ, а именно: Программа ЕС "За более безопасный интернет", Европейское Агентство по безопасности сетей и информации (ENISA)[3], Детская благотворительная коалиция за безопасность интернета, инициатива Киберпространство и Эдинбургский университет (Соединенное Королевство). Кроме того, бесценные вклады были получены от отдельных национальных правительств и высокотехнологичных компаний, которые разделяют общие идеи о том, как сделать интернет более безопасным и более хорошим местом для детей и молодежи.

МСЭ вместе с другими авторами этого отчета призывают все заинтересованные стороны способствовать принятию правил и стратегий, которые будут защищать детей в киберпространстве и содействовать созданию безопасного доступа к онлайновым ресурсам.

Это приведет не только к построению всеохватывающего информационного общества, но также позволит Государствам – Членам МСЭ выполнить свои обязательства по защите и обеспечению прав детей, которые прописаны в Конвенции ООН по правам ребенка[4], утвержденной резолюцией 44/25 Генеральной Ассамблеи ООН 20 ноября 1989 года, и в Заключительных документах ВВУИО[5].

[3] http://www.enisa.europa.eu

[4] http://www.unicef.org/crc

[5] http://www.itu.int/wsis/outcome/booklet.pdf

Руководящие указания для родителей, опекунов и учителей

Цель этого раздела – предоставить руководящие указания для родителей, опекунов и учителей, для того чтобы они могли помочь детям оставаться в безопасности, находясь в онлайновом режиме и получить положительный опыт. Более подробный перечень пунктов, которые необходимо рассмотреть, приведен на странице 49.

Родители, опекуны и учителя		
	№	**Основные аспекты, требующие внимания**
1 Защита и безопасность вашего персонального компьютера	a	Поставьте компьютер в общей комнате
	b	Установите брэндмауэр и антивирусное программное обеспечение
2 Правила	a	Договоритесь о правилах использования интернета и персональных устройств дома, обращая особое внимание на проблемы секретности: места, неподобающие для детского возраста, запугивание и опасности со стороны незнакомцев
	b	Договоритесь о правилах использования мобильных устройств
3 Обучение родителей, опекунов и учителей	a	Родители, опекуны и учителя должны быть хорошо знакомы с интернет-сайтами, используемыми их детьми, и должны хорошо понимать, как дети проводят время в онлайновом режиме
	b	Родители, опекуны и учителя должны понимать, как дети используют другие персональные устройства, такие как мобильные телефоны, игровые консоли, MP3-плееры, PDA и т. д.

Родители, опекуны и учителя		
	№	**Основные аспекты, требующие внимания**
4 Обучение детей	a	Говорите своим детям о рисках, связанных с сообщением персональной информации; о личных встречах с людьми, с которыми они познакомились в онлайновом режиме; о помещении фотографий в онлайновый доступ; об использовании веб-камер и т. д.
5 Общение	a	Рассказывайте своим детям о собственном опыте

1. Общие сведения

Всемирная встреча на высшем уровне по вопросам информационного общества (ВВУИО), которая проходила в два этапа в Женеве (10–12 декабря 2003 года) и в Тунисе (16–18 ноября 2005 года), завершилась четко выраженным обязательством – "построить всеобъемлющее, ориентированное на потребности людей и на цели развития, информационное общество, в котором каждый может создавать, получать доступ, использовать и делиться информацией и знаниями" (Женевская Декларация принципов, параграф 1).

На ВВУИО лидеры международного сообщества, утвердив Направление действий С5, поручили МСЭ "создание доверия и безопасности при использовании ИКТ".

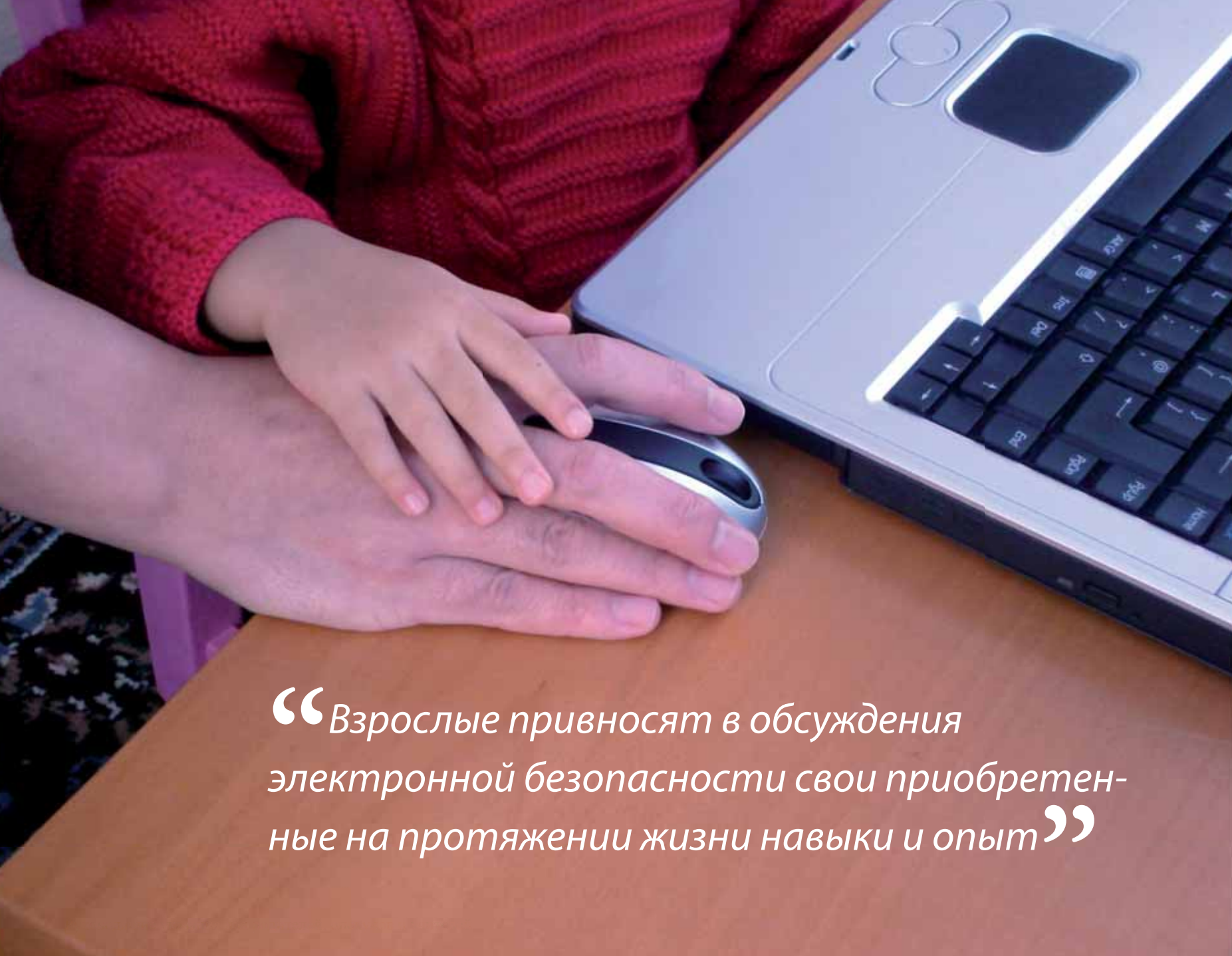
В заключительных документах ВВУИО также отдельно признаются права детей и молодежи, и их защита в киберпространстве.

Тунисское обязательство признало "роль информационно-коммуникационных технологий (ИКТ) в деле защиты детей и в расширении развития детей". А также потребность "укрепления действий по защите детей от эксплуатации и охране их прав в условиях ИКТ".

Как правило, подразумевается[6], что обычно мы знаем, где бывают наши дети каждый день, с кем они, и что они делают.

Но в цифровом мире, где даже самые младшие наши дети проводят все больше времени, наша роль часто сводится просто к

[6] http://www.parenting.com/article/Mom/Relationships/How-to-Spy-on-Your-Child-Online



“Взрослые привносят в обсуждения электронной безопасности свои приобретенные на протяжении жизни навыки и опыт”

роли наблюдателя, и многих из нас лихорадит от одной мысли о "цифровой угрозе".

Дети, даже очень маленькие, могут очень хорошо понимать современную технологию, лучше чем их учителя или родители.

Дети сегодня знают только тот мир, который кибернетизирован, в котором технология вплетена в каждый аспект их жизни.

Она наполняет информацией их дружбу, образование и их понимание окружающего мира и людей. В то же время, мы взрослые размышляем о том, какие правила установить и как добиться их выполнения.

Проблема состоит в том, что этот конкретный предмет не освещен в книге для родителей, эта глава еще не написана, и у общества нет времени сформировать стандарты.

У нас установлен законом возраст, с наступлением которого разрешается потребление спиртных напитков, и возраст, с наступлением которого разрешается водить автомобиль, но нет никаких авторитетных рекомендаций о возрасте, с которого дети могут безопасно самостоятельно выходить в интернет, или писать текстовое сообщение другу на своем сотовом телефоне, или о том, что задача родителей наблюдать за нашими уязвимыми и часто наивными детьми во время их онлайновых действий.

Существует дезориентирующий разрыв между тем, что думают родители о том, что знают их дети, и тем, что дети на самом деле знают.

Тогда как 92% родителей говорят, что они установили правила для онлайновых действий своих детей, 34% детей говорят, что их родители этого не делают.

В разных странах мира эти цифры похожи:

Во Франции 72% детей находятся в интернете без присмотра, при этом 85% родителей только знают о программном обеспечении для "контроля со стороны родителей", и всего лишь 30% его установили.

В Корее 90% домов имеют выход в недорогой широкополосный интернет, и до 30% корейцев в возрасте до 18 лет подвергаются риску интернет-привязаннсти, проводя в онлайновом режиме по два часа в день и более.

В Соединенном Королевстве 57% людей в возрасте 9–19 лет говорят, что они смотрели онлайновую порнографию, 46% говорят, что они распространили информацию, которую не должны были передавать, и 33% говорят, что их запугивали в онлайновой среде.

В Китае 44% детей говорят, что в онлайновом режиме к ним обращались незнакомцы, и 41% вели разговоры с одним онлайновым незнакомцем о сексе или о чем-то, что заставляло их ощущать неудобство.

В целях нахождения решения для этих нарастающих проблем МСЭ вместе с другими заинтересованными сторонами в ноябре 2008 года запустил инициативу "Защита ребенка в онлайновой среде" (COP)[7].

Инициатива COP была разработана МСЭ как часть Глобальной программы действий по кибербезопасности (GCA)[8] и сформирована как международная сеть

[7] www.itu.int/cop

[8] www.itu.int/osg/csd/gca

сотрудничества для действий по содействию всемирной защите детей и молодежи в онлайновом режиме путем предоставления руководящих указаний по безопасному поведению в он-лайне совместно с другими агентствами и партнерами ООН.

Ключевыми целями инициативы COP являются:

- определить основные риски и уязвимые места для детей и молодежи в киберпространстве;
- повысить уровень информированности о рисках и проблемах с использованием множества информационных каналов;
- разработать практические средства помощи правительствам, организациям и учебным заведениям с целью минимизации рисков;
- обмен знаниями и опытом в целях содействия международному стратегическому партнерству в определении и реализации конкретных инициатив;
- эти Руководящие указания подготовлены в рамках инициативы МСЭ "Защита ребенка в онлайновой среде (COP)" и имеют своей целью предоставление родителям, опекунам и учителям информации, советов и подсказок по безопасности в сфере защиты ребенка в онлайновой среде.

2. Дети и молодые люди он-лайн

Последние годы интернет продолжает стремительно меняться. Новые службы, такие как блоги, Wikipedia, My Space, You Tube и онлайновые игры еще больше повысили соединение с интернетом, стимулируя общение и позволяя пользователям создавать собственный контент. В течение последних двух лет количество новых блогов продолжает удваиваться каждые пять месяцев; использование веб-сайтов социальных сетей, таких как Bebo, Facebook, Habbo и Twitter увеличивается год от года; и за последние три года общение между пользователями Всемирной паутины стало самым крупным источником интернет-трафика.

Дети и молодые люди активно и увлеченно используют ИКТ для таких целей как чат или обмен персональной информацией. Это создает массу хороших возможностей для участия, творчества и образования. Это также позволяет молодым людям общаться без государственных, религиозных или культурных границ. Например, в следующей таблице описан тип онлайновых действий, которые наиболее вероятно будут осуществлять дети при получении доступа к виртуальным мирам[9]:

[9] ENISA, Дети в виртуальных мирах - Что следует знать родителям, сентябрь 2008 г., доступен по адресу: http://www.enisa.europa.eu/doc/pdf/deliverables/дети_on_virtual_worlds.pdf

Тип игрока	Интересы	Это вероятно	Характеристики
Исследователи-разведчики	Выполнение квеста, разгадка загадочных событий, путешествия, времяпрепровождение вне дома	Более уверенные в себе дети, без различия по полу и возрасту	Изучают подробности. Любознательны и общительны, обладают воображением, увлечены тайнами
Самовыразители	Представление самого себя в мире	Возможно, более старшие дети, обоих полов	Мальчики и девочки желают "отразить себя" в своем персонаже, возможно дать ему свое лицо; старшие девочки хотят одевать своих персонажей и делать им макияж. Как мальчики, так и девочки стремятся выразить себя, создавая дом или "базу"
Карьеристы	Повышение рейтинга, социальной позиции в обществе	Как маленькие, так и старшие дети; с небольшим гендерным перекосом (мальчики подвержены несколько больше, чем девочки)	Конкурентные, заинтересованные в рейтингах и демонстрации своего положения окружающим
Бойцы	Смерть и разрушение, жестокость, сверхспособности	Мальчики, с некоторым перекосом в сторону старших мальчиков	Дети чувствуют безысходность, когда не имеют возможности самовыражения; наличие возможности обыграть или поразить соперника уменьшает чувство безысходности

Тип игрока	Интересы	Это вероятно	Характеристики
Коллекционер-потребитель	Накапливает что-либо ценимое в системе	Старшие мальчики и девочки	Коллекционирует страницы и монеты, ищет магазины, создает возможности, средства и места для размещения своих сокровищ
Опытные пользователи	Со всеми делится своими знаниями и своим опытом	Эксперт в играх, географии окружающего мира, системах	Проводит в он-лайне по нескольку часов в день, играя и исследуя игру, проявляя глубокий интерес к тому, как работает игра
Создатели жизненных систем	Создание новых земель, новых элементов окружающего мира, населения окружающей среды	Младшие дети (воображаемый мир без каких-либо правил), и старшие дети (воображаемый мир с правилами и системы: дома, школы, магазины, транспорт, экономика)	Дети чувствуют безысходность, когда не имеют возможности самовыражения; создаются системы (или их отсутствие) для управления окружающей средой
Воспитатели	Забота о своем персонаже или питомцах	Маленькие мальчики и девочки и старшие девочки	Дети стремятся знакомиться и играть с другими детьми, обучать своего персонажа таким навыкам как плавание и иметь место, где их персонаж спит. Также появляются виртуальные питомцы

Интернет – это нейтральный инструмент для распространения информации, которая может быть использована как с благородными, так и со злонамеренными целями.

С одной стороны, например, он имеет громадный потенциал, как источник образования для людей всех возрастов и с разными возможностями.

Тогда как с другой стороны, интернет может использоваться для расстановки онлайновых ловушек с целью использования пользователей в преступных целях и, к несчастью, дети находятся среди тех, кто наиболее уязвим для таких ловушек.

Важно помнить, что интернет – не единственное средство общения, которое может отрицательно влиять на благополучие детей.

За последние несколько лет использование молодыми людьми мобильных телефонов значительно выросло, и дети используют свои мобильные телефоны для доступа в интернет практически из любого места, где они бывают.

Это повышает вероятность того, что без надзора взрослых они будут подвергаться онлайновой опасности.

В Корее, например, средний возраст детей, которые получают свой первый мобильный телефон, составляет примерно восемь лет.

Важно помнить, что в последнее время и сами мобильные телефоны развиваются.

Сегодня телефоны могут быть использованы для передачи видеосообщений, развлекательных услуг (скачивание игр, музыки и видеопрограмм), а также для доступа в интернет с целью получения местных услуг, зависящих от местоположения.

Потенциальные риски для детей, получивших доступ в интернет через мобильные телефоны или другие персональные устройства, аналогичны тем, которым они подвергаются, выходя в интернет через проводное соединение.

Большая разница между доступом ребенка в интернет с мобильного телефона и традиционного доступа с домашнего компьютера заключается в том, что такие мобильные персональные устройства являются личной вещью.

В тех случаях, когда используются персональные устройства, главным образом, подростками, родители, как правило, не могут непосредственно наблюдать за ними, как это может быть сделано с домашним компьютером.

Родителям следует беседовать со своими детьми об использовании таких устройств, и в момент покупки или первого использования убедиться в том, что они имеют контроль над устройствами своих детей.

Ситуативное исследование: Египетская молодежь и интернет

Целевая группа по безопасности интернета для египетской молодежи (Net-Aman) состоит из 11 членов от 18 до 28 лет, и входит в состав более широкой инициативы КиберМир, разработанной Международным женским движением за мир Сюзанны Мубарак при поддержке целого спектра партнеров.

Название целевой группы Net-Aman (по-арабски "Безопасность сети") было выбрано всеми ее молодыми участниками.

Задачи этой группы заключаются в повышении осведомленности о безопасности интернета и огромном потенциале ИКТ, с тем чтобы предложить детям и молодежи возможность самостоятельно определять вредоносный контент и выбирать наилучший способ обращения с ним, при этом выбран подход, предполагающий их активное участие.

Первая учебная сессия группы Net-Aman сформировала вопросник, который используется членами группы для получения "статистического представления" о детях и молодежи, стремящихся и надеющихся использовать интернет в Египте.

Каждый молодой участник группы получил задание идти в школы или университеты и на второй учебной сессии в марте 2008 года представить отчет о результатах сделанного обзора. Обзор охватывает различных молодых людей и представляет различные возрастные группы от 8 до 22 лет.

Такой обзор помог группе Net-Aman понять, что думают молодые люди в Египте об интернете и о своей безопасности.

Примерно 800 египетских молодых людей ответили на опрос "youth2youth" с названием "Египетская молодежь и интернет".

Участвующие в обзоре дети и молодые люди утверждали, что:

- Взрослые не наблюдают за ними во время использования интернета.
- Отвечая на вопрос о рисках и проблемах интернета в Египте, они перечислили следующее: основной риск представляет собой недопустимый контент, затем вирусы и шпионские программы, жестокий контент, копирование для выполнения домашних работа (плагиат), и на последнем месте названо киберзапугивание.
- Одним из наиболее шокирующих результатов обзора был тот факт, что самые молодые сообщают в интернете свою персональную информацию, полное имя, возраст, фотографии, информацию о школе и телефонные номера, совершенно не беспокоясь о последствиях.

В свете результатов этого обзора и в соответствии с мандатом Целевой группы по безопасности интернета для египетской молодежи (Net-Aman), молодые участники группы будут продолжать вносить свой вклад и участвовать в мероприятиях, способствующих повышению осведомленности египетской молодежи о проблемах защиты ребенка в онлайновой среде.

Для получения дополнительной информации, посетите веб-сайт инициативы Киберпространство http://www.smwipm.cyberpeaceinitiative.org.

3. Родители, опекуны и учителя

Определение родителей, опекунов и учителей

Несколько интернет-сайтов употребляют слово родители в общем смысле, например, на "странице родителей" или " родительский контроль", следовательно, было бы полезно определить людей, которые в идеале должны гарантировать, что дети безопасно используют интернет-сайты, дают разрешение на использование конкретных интернет-сайтов и чувствуют за это ответственность.

В этом документе термином "родители" будем называть естественных мать и/или отца ребенка, или человека, которому были даны права опекунства.

В сегодняшнем мире известно огромное количество случаев, когда о детях заботятся люди, не являющиеся их естественными родителями.

Их часто называют опекунами или воспитателями, и очень важно обязательно понимать роль, которую они могут играть, когда дети, за которых они отвечают, находятся в он-лайне.

Учитель – это человек, который систематически работает с целью улучшения понимания другим человеком определенного предмета.

Роль учителя исполняют и те, кто ведет занятия в классе, и более неформальные учителя, которые работают, например, на сайтах

социальных сетей, где предоставляют информацию об онлайновой безопасности, или руководят сообществами, или школьными курсами, позволяющими детям оставаться в безопасности, находясь в он-лайне.

Работа учителей будет меняться в зависимости от условий, в которых они работают, и от возрастной группы детей (или взрослых), которых они стараются научить.

Все, кто вступает в контакт с детьми и молодыми людьми, родители, учителя, социальные работники, библиотекари, работники службы семьи, молодежные лидеры и другие члены семьи, включая дедушек и бабушек. Важно отметить, что дети, находящиеся под опекой социальных служб, являются особенно уязвимой группой и, следовательно, нуждаются в особом внимании.

Кроме того, важно рассмотреть роль наблюдения со стороны ровесников, поскольку они также являются учителями в одном из смыслов этого слова.

Чего не знают многие родители, опекуны и учителя

Недавний анализ, проведенный ENISA, показал, что в большинстве случаев родители и опекуны не знают в подробностях о том, с чем могут столкнуться их дети в он-лайне, а также о рисках и уязвимых точках, связанных с различными онлайновыми действиями.

Дети могут находиться в он-лайне, используя различные платформы и устройства, среди которых могут быть:

1. персональные компьютеры,
2. мобильные телефоны,
3. персональные цифровые помощники (PDA).

В зависимости от типа используемой платформы и доступных функций, каждый человек приобретает свой собственный опыт. Например:

Функция	Описание
Создание профиля	Ввод информации о самих пользователях.
Взаимодействие с другими людьми	Обсуждение информации и идей с другими пользователями в чате, блогах, посредством мгновенных сообщений, форумов и функций передачи речи по Протоколу интернет (VoIP).
Создание аватара	Выбор графического изображения, которое представляет пользователя и является его идентификатором на интернет-сайте.
Игры	Решение проблем и выполнение действий, участие в онлайновых играх.
Решение задач	Задачи на развитие интеллекта, как правило, с получением некоторого приза за участие. Кроме того, они дают возможность соревнования между друзьями или группами друзей в форме команд.
Создание графики, анимационных фильмов, комиксов и гаджетов	Также называется контентом, создаваемым пользователями (UGC = User-Generated Content), многие дети очень любят создавать свой собственный контент и демонстрировать его в своем сообществе, и их творчество расцветает при взаимодействии с другими участниками виртуального сообщества.
Создание широкого спектра контента от музыки и танцев до видеороликов	Самостоятельная публикация допускается для людей всех возрастов и может стать отличным выходом для творческого потенциала.
Покупка продуктов	Некоторые сервисы могут давать пользователям возможность покупать продукты или услуги за реальные деньги.
Загрузка в интернет фотографий или любой другой информации	Некоторые сервисы могут давать детям возможность загружать в интернет фотографии или видеоинформацию. Некоторые сервисы фильтруют персональную информацию и/или другой неприемлемый контент.
Скачивание музыки	Некоторые сервисы могут давать детям возможность скачивать из интернета музыку.
Просмотр рекламы продуктов/услуг	Интернет-сайты часто финансируются за счет размещения рекламы.

Молодые люди выходят в интернет по множеству различных причин, включая следующие[10]:

1 Взаимодействие с друзьями в новых условиях в реальном времени, обмен мнениями в сфере общих интересов с другими.
2 Создание и присоединение к сообществам или группам по интересам, например, музыка, футбол и т. д., общение на темы информации из сферы общих интересов в блогах, посредством мгновенных сообщений и других инструментов.
3 Знакомство с новыми людьми и, конечно же, с новыми друзьями.
4 Создание и передача оригинального и персонального контента, такого как изображения, фотографии и видеоролики, для расширения возможностей самовыражения.
5 Создание, публикация и обмен музыкой.
6 Игра в игры.
7 Создание собственного пространства, даже в присутствии родителей и воспитателей.
8 Эксперименты со своими личными данными, новым пространством для общения и социальными границами.

Даже если опыт пользователей различен, в том случае, когда он выходит в интернет с мобильного телефона или PDA, а не с персонального компьютера, риски и уязвимости, связанные с использованием интернета, одинаковы вне зависимости от платформы.

Одной из ключевых проблем является то, что дети и молодые люди стремятся выходить в интернет из тех мест, о которых мы сказали им, что они безопасны, т. е. из дома и школы. Родители и опекуны имеют аналогичные ошибочные представления и часто говорят, что они предпочитают, чтобы их дети использовали компьютер дома, а не где-либо еще, когда родители не знают об их местонахождении. Несомненно, интернет может перенести детей и молодых людей в любое место, где они могли бы подвергаться рискам точно таким же, как это могло быть в реальном мире. (смотрите, страницу 21).

[10] Home Office, Целевая группа Home office по защите ребенка в интернете – Руководство хорошего опыта для провайдеров социальных сетей и других интерактивных услуг, 2008 г., доступен по адресу: http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance?view=Binary (последний раз посещался 16 июня 2008 года).

Ситуативное исследование: Секретность в опасности

Многие пользователи не знают не только о том, как много персональной информации разглашают они в онлайновом режиме, но даже и о том, как это они делают! Такие методы включают в себя:

- забывание поставить галочку в графе "данные засекретить"; и
- разглашение больше информации, чем требуется.

Однако дети и молодые люди остаются уязвимыми для (возможно) неприемлемых контактов с ровесниками, старшими подростками или даже взрослыми. Дети могут также несознательно разглашать информацию о себе посредством:

- заполнения формы любого типа, например, на конкурсе или при регистрации;
- размещения персонального профиля;
- создания веб-сайта.

Важно, чтобы родители не преувеличивали риски или не пугали детей чрезмерно, когда мы обсуждаем риски, которые могут встретиться в он-лайне.

Знание о том, каким образом дети могут несознательно разглашать информацию в он-лайне и насколько просто незнакомцы могут отыскать информацию о них, является одной из важнейших вещей, которые требуется учитывать.

Дети должны знать, что существует множество баз данных, которые могут предоставить информацию об их адресе, номере телефона и адресе электронной почты. Детям и молодым людям следует стремиться использовать секретные настройки каждый раз, когда находятся в онлайне и сообщать ответственному взрослому, если у них спрашивают данные о персональной (физической) информации или онлайновое общение становится для них неприятным.

Ниже приводится учебная дискуссия в одной из комнат чата, которая, как уверены служащие правоохранительных органов, являются вполне реалистичным примером онлайновых дискуссий. Вообразите, что интернет-хищник педофил сидит и делает заметки относительно этого ребенка, и использует эту информацию, для того чтобы заманить его позже. Поддастся ли на такое ваш ребенок? К несчастью, кто-то поддастся.

Ребенок: Я ненавижу свою мать! Я знаю, это она виновата в том, что родители развелись.

Интернет-хищник: Я знаю. Мои родители тоже развелись.

Ребенок: У нас больше никогда не будет денег. Каждый раз, когда мне что-то надо, она говорит одно и тоже: "Мы не можем себе этого позволить". Когда мои родители были вместе, я мог покупать вещи. Теперь я не могу.

Интернет-хищник: Я тоже.

Я ненавижу это!

Ребенок: Я шесть месяцев ждал, когда выйдет новая компьютерная игра. Мама обещала купить ее мне, когда она

появится. Она обещала! Теперь она вышла! Я могу купить ее? Нет. "У нас не хватает денег!" Я ненавижу свою мать!

Интернет-хищник: О! Мне так жаль! Я понял! У меня есть крутой дядюшка, который мне всегда покупает вещи. Он очень богат.

Ребенок: Везет тебе. Я бы хотел иметь богатого и крутого дядю.

Интернет-хищник: Эй! У меня идея! Я спрошу дядю, что если я тебе куплю тоже.... Я говорю, он действительно крутой. Я уверен, что он скажет да.

Ребенок: Правда!? Спасибо!!

Интернет-хищник: BRB [сокращение выражения "be right back" = сейчас вернусь] . . . пойду ему позвоню.

Интернет-хищник: Знаешь, что? Он сказал – ОК. Он купит тебе игру!

Ребенок: О, правда? Спасибо. Не могу поверить!!!

Интернет-хищник: Ты где живешь?

Ребенок: В Нью-Джерси, а ты?

Интернет-хищник: В Нью-Йорке. И мой дядя – тоже. Нью-Джерси – недалеко.

Ребенок: Класс!

Интернет-хищник: Около твоего дома есть торговый центр? Можем встретиться там.

Ребенок: ОК. Я живу возле торгового центра GSP.

Интернет-хищник: Я слышал о нем. Нет проблем. Как насчет субботы?

Ребенок: Круто.

Интернет-хищник: Мы можем пойти в Макдональдс, если хочешь. Мы тебя там встретим в полдень.

Ребенок: ОК. Где?

Интернет-хищник: Перед магазином компьютерных игр. Да! Дядю зовут Джордж. Он на самом деле крутой.

Ребенок: Класс . . . спасибо, я так благодарен. Тебе очень повезло, что у тебя такой богатый и крутой дядя.

Наступает суббота, ребенок идет в торговый центр и встречает взрослого человека около магазина компьютерных игр. Тот представляется как "Дядя Джордж" и говорит, что его племянник уже ждет их в Макдональдсе.

Ребенку неудобно, но дядя идет в магазин и покупает игру за 100 долларов. Он выходит и отдает ее ребенку, который сразу успокаивается и радуется.

Предупреждение об опасности встречи с незнакомцем здесь не сработает. Это – не незнакомец. Это "Дядя Джордж", и если нужны еще доказательства, то есть компьютерная игра. Он садится в машину Дяди Джорджа, не сомневаясь, что встретит своего друга в Макдональдсе. Остальное будет рассказано в шестичасовых новостях.

Это ужасно. Нас от этого наизнанку выворачивает, но это случается. Не очень часто, но достаточно часто, и вы должны быть предупреждены заранее. (Несколько сотен киберпреступников ловят и арестовывают каждый год.) Хотя, даже одного – слишком много, если это ваш ребенок. Знания о том, как они действуют и какие трюки используют, поможет вам научить своего ребенка тому, как не стать их жертвой.

Источник: http://www.wiredkids.org/parents/parry_guide.html

Онлайновые риски и уязвимые места, связанные с использованием интернета

Подверженность воздействию незаконного и вредного контента, такого как порнография, азартные игры и другого неприемлемого для детей, и контакты с другими пользователями. В большинстве случаев операторы этих сайтов не принимают эффективных мер для ограничения доступа детей к своим веб-сайтам.

Создание, прием и распространение незаконного и вредного контента.

Злоумышленник выдает себя за другого, часто за другого ребенка, в явной попытке обидеть кого-либо, домогаясь или запугивая его.

Нежелательный контакт, особенно когда взрослые люди, выдают себя за других, или представляются детьми.

Раскрытие персональной информации, приводящее к риску физического насилия.

Преступные попытки выдать себя за другого пользователя интернета, главным образом для получения финансовых выгод. В некоторых случаях они могут включать в себя кражу идентичности, хотя, как правило, кража идентичности связана с попытками обмануть взрослых.

Физическое насилие в реальной жизни пересекается с онлайновыми знакомствами, причем появляется возможность сексуального насилия.

Целенаправленная обработка при помощи спама и рекламы от компаний, использующих интернет-сайты с целью продвижения продуктов для людей определенного возраста или определенных интересов.

Интенсивное использование для причинения ущерба социальных мероприятий и/или активного отдыха, важного для здоровья, укрепления доверия, социального развития и общего благополучия.

Запугивание и насилие.

Причинение ущерба самому себе, разрушительное и жестокое поведение различного типа, например, "Радостное избиение" (happy slapping).

Маниакальное или чрезмерное использование интернета или онлайновых игр. Подверженность расизму или другим дискриминационными текстам или изображениям.

Диффамация и разрушение репутации.

Несоблюдение собственных прав или прав других людей в процессе плагиата и загрузка в интернет контента, в частности фотографий. Показано, что скачивание и загрузка в интернет фотографий неподобающего содержания без разрешения может причинять вред другим людям.

Несоблюдение авторских прав других людей, например, путем скачивания из интернета музыки, фильмов или ТВ программ, за которые следовало бы заплатить.

Использование найденной в онлайне неточной или неполной информации или информации из неизвестных или ненадежных источников. Несанкционированное использование кредитных карт: кредитных карт родителей или других людей для оплаты членских взносов, оплаты других услуг или для покупки товаров.

Ложное указание возраста: либо ребенок выдает себя за человека более старшего возраста с целью получения доступа к сайтам, не соответствующим его возрасту, либо взрослые люди выдают себя за детей по тем же причинам.

Использование электронного адреса родителей без их согласия: когда для активации учетных записей детей в виртуальном мире требуется согласие родителей, дети могут злоупотреблять доступом к учетным записям родителей. В некоторых службах родители не имеют возможности просто удалить свои учетные записи после того, как они активированы.

Нежелательная реклама: некоторые компании через сайты виртуальных миров шлют детям спамовые рекламные сообщения, приглашая купить товары. Все это поднимает вопрос о согласии пользователя

и о том, как его следует получать. Законодательство в этой области несовершенно, и очевидно, что очень сложно определить, когда дети способны понимать процесс передачи данных. Кроме того, вопрос о том, как применять эти правила в интернете, уже вызывает серьезное беспокойство, и доступ с мобильных телефонов еще больше выделяет эту проблему.

В частности, далее представлены вопросы, вызывающие наибольшую озабоченность учителей, поскольку они чувствуют, что не имеют достаточной квалификации для того, чтобы справиться с ними:

Социальные сети – способ, посредством которого проводят часть жизни дети и молодые люди, используя социальные миры, значительно отличается от того, с чем знакома большая часть учителей. Многие не могут понять, почему так важно иметь такое количество "друзей" или такой обширный список контактов, но для молодых пользователей число друзей представляется равнозначным популярности.

Загрузка в интернет обнаженных фотографий – относительно новое явление, когда дети и молодые люди подвергают себя риску, размещая он-лайн свои сексуально провоцирующие изображения или посылая их друзьям, используя технологии мобильного доступа.

Как дети используют новые средства информации отличается от того, что мы думаем на этот счет. Имеются несколько хороших исследований в отдельных странах, которые могут помочь этой работе. Смотрите также сайт EU Kids Online, где можно найти данные о проблемах Европейского союза, рисках и т. п., по адресу: www.eukidsonline.net).

Куда обратиться за помощью? Во многих странах есть службы помощи, куда дети и молодые люди могут сообщить о проблеме. Информация о них широко распространена, и в разных странах используются различные подходы для получения этих сообщений. Важно, чтобы дети и молодые люди понимали, что никогда не поздно сообщить о проблеме и что, сделав это, они помогают другим.

Как учителя подвергаются риску запугивания, например, со стороны детей и молодых людей, которые создают отвратительные сайты об учителях и других работниках. Учителя должны быть уверены в том, что они используют технологию безопасным образом. Многие чувствуют, что не имеют достаточной квалификации для того, чтобы справиться с некоторыми такими проблемами, и не знают, как убрать материал с сайтов и т. д. Веб-сайт "teachtoday" дает несколько отличных рекомендаций по этому поводу, а также по другим связанным проблемам. www.teachtoday.eu.

Важно подчеркнуть, как указано выше, что, несмотря на то, что некоторые учителя не являются также хорошо образованными технически, как дети и молодые люди, но они обладают хорошими навыками и жизненным опытом, и могут дать совет, рекомендацию или предоставить поддержку. Учителям следует это многократно повторять во время обучения по вопросам электронной безопасности.

Исследование OPTEM[11], однако, полагает, что риски, определенные детьми самостоятельно, больше связаны с интернетом, чем с мобильными телефонами, и включают в себя:

Риски для компьютера, например, вирусы и хакерские атаки.

Незапрашиваемое появление изображений или ошибочный доступ к нежелательным веб-сайтам, на которых показано насилие или порнография. (Более старшие дети стремятся уменьшить влияние случайного воздействия.)

Обман и мошенничество.

Мошеннические и обманные сексуально-ориентированные атаки со стороны злонамеренных взрослых.

[11] http://ec.europa.eu/информация_society/activities/sip/docs/eurobarometer/qualitative_study_2008/summary_report_en.pdf

Хотя дети осознают, что они иногда ведут себя рискованно, они не проявляют большого беспокойства относительно возможных рисков поведения такого типа и предпочитают решать проблемы самостоятельно или с помощью ровесников. Это предполагает, что они обратятся к своим родителям или другим взрослым только в случае потенциально "ужасных" проблем. Эта проблема особенно присуща старшим мальчикам, которые может быть более вероятно используют кнопку аварийного вызова[12], например, такую как разработанная Целевой группой Virtual Global. Однако это сделают не все дети. Мы видим, что дети, которым известно о рисках, "контролируют" свои собственные действия, но часто не разделяют той точки зрения на новые технологии, которая предполагает, что поведение молодых людей должно оцениваться и контролироваться взрослыми[13]. Мы должны быть осторожными, делая простое различие между реальным и онлайновым мирами, поскольку наша ежедневная жизнь становится все больше связанной с онлайновыми технологиями. Для многих детей эта связь означает осторожные согласования между возможностями, предоставляемыми новыми технологиями, например, изучение собственной идентичности, создание тесных дружеских взаимоотношений и расширенные возможности для общения, и рисками в отношении секретности, неправильного понимания и методов злонамеренного использования, предлагаемых средствами связи, связанными с интернетом[14].

Одна роль для всех?

Важно помнить, что для детей и молодых людей основную поддержку в изучении оказывают учителя и родители[15].

В Отчете Byron[16] (Соединенное Королевство) предполагается, что правила защиты ребенка должны включать в себя кампанию по повышению осведомленности, которая обеспечивает обучение взрослых: родителей, учителей, опекунов, которые могут не быть знакомы с технологией, а также обучение детей, с тем чтобы они стремились использовать меры безопасности или не подвергали себя лишним рискам.

Правильные сообщения для правильных людей

Основная цель такой кампании состоит в том, чтобы изменить поведение детей, включая стимулирование более безопасного поведения в сети, и эффективных действий со стороны родителей и других людей, которые взаимодействуют с детьми, это могут быть другие члены семьи, учителя и т. д. по обучению детей тому, как оставаться в безопасности, находясь в он-лайне.

Безопасность детей в интернете следует рассматривать не как отдельную проблему, а как проблему, имеющую общие параметры в различных инициативах, касающихся детей, их безопасности и интернета.

[12] http://www.virtualglobaltaskforce.com/

[13] Quayle, E., Lööf, L. & Palmer, T. (2008), Child Pornography and Sexual Exploitation Of Children Online. Bangkok: ECPAT

[14] Livingstone, S. Taking risky opportunities in youthful content creation: teenager's use of социальные сети sites for intimacy, privacy and self-expression. New Media and Society, 10 (3), 2008 г., 393-411.

[15] Livingstone, S., Bober, M. UK Children Go Online, Final report of key project findings, апрель 2005 года

[16] Byron, T. (2008) Safer Children in a Digital World.

Роль, которую могут играть родители и опекуны

Для гарантии того, что дети используют интернет-сайты безопасно и ответственно, родители и опекуны могут:

1 Разговаривать со своими детьми о том, что они делают и с кем они общаются, когда используют компьютер или персональное устройство, например, мобильный телефон или игровую консоль. Открытость и поддержание таких диалогов очень важны для обеспечения безопасности детей.

2 Читать со своими детьми правила и условия применения сайта до захода на него, обсуждать вместе с ними меры безопасности, установить некоторые базовые правила и контролировать использование, с тем чтобы быть уверенным, что эти правила соблюдаются.

3 Научить юных пользователей ответственному использованию технологий вообще, объясняя им, что нужно прислушиваться к собственным инстинктам и пользоваться здравым смыслом.

4 Проверять, используют ли сайты такие технические решения как:

- Фильтры и родительский контроль.
- Сохранение истории деятельности пользователя.
- Модерация, и если она есть, осуществляется ли она человеком или автоматически, например, с использованием фильтрации текста, которая распознает определенные образцы текста и URL? Используется ли на сайте комбинация вмешательства человека и автоматических инструментов? Модераторы – это люди, которые специально обучаются тому, чтобы обеспечить безопасную и соответствующую среду. Активные модераторы часто изображаются как персонажи или участники виртуального мира или, в условиях игры могут действовать как хозяин игры, в каждом случае они видны всем пользователям. Обычно модератор игры вмешивается, только когда возникает сложная ситуация, но в некоторых играх они помогают пользователям, которые "потерялись" или нуждаются в помощи. Молчаливые модераторы, обычно, остаются на заднем плане, блокируя запретный материал, реагируя на подозрительное поведение, предупреждая пользователей и выполняя другие полицейский функции.
- Если на сайте разрешена загрузка фотографий или видеороликов, то выполняется ли на сайте активная их модерация, или изображения на нем просматривают только, получив сообщение о размещении несоответствующего контента?
- Функции сообщения и блокировки: обычно это доступные инструменты для сообщения о размещении несоответствующего контента, диалогах и действиях, например "флаги" и "кнопки сообщений". Кроме того, в виртуальном мире должны быть ясно показаны правила того, как и кому сообщать о несоответствующем поведении. Детей следует научить сообщать о происшествиях или о нежелательных контактах и о том, как блокировать нежелательные контакты, использовать установки конфиденциальности и как записывать онлайновые разговоры.
- Рейтинги: родители и опекуны должны быть осведомлены о символах рейтинга и их использовании, как о важном инструменте для защиты молодых пользователей от несоответствующих служб и контента.

- Подтверждение возраста: если сайт объявляет об использовании системы подтверждения возраста, то насколько надежны его системы? Если продаются продукты для ограниченного возраста, используется ли надежная система подтверждения возраста для подтверждения возраста конкретного лица?

5 Участвовать в онлайновых действиях маленьких пользователей. Очень важно понимать важность той роли, которую родители и воспитатели могут и должны играть на интернет-сайтах. Потому что их участие оказывает мощное влияние на опыт, получаемый детьми и способствует положительному поведению.

6 Сохранять спокойствие и не делать скоропалительных выводов, если вы слышите или видите что-то беспокоящее вас в поведении вашего ребенка или в поведении одного из его онлайновых друзей. Некоторые интернет-сайты для некоторых молодых людей являются местом их общественной жизни. Если ваши дети испугаются, что вы просто отключите их связь с социальной жизнью, они, по всей вероятности, будут все меньше делиться с вами проблемами и опасениями, которые могут у них возникать.

7 Знать, что ваш ребенок может вести себя совершенно иначе в он-лайне, чем в реальном мире, когда он с вами. Часто бывает, что люди более агрессивны в он-лайне, где, как им кажется, они ни за что не отвечают. Использование вашим ребенком отчетов о неподходящем поведении является возможностью обсудить с ребенком, каким должен быть приемлемый тон для онлайновых обсуждений.

8 Изучать онлайновую культуру, таким образом вы сможете понимать смысл типовых отговорок, используемых молодыми людьми, которые встречаются с необходимостью отвечать за свое поведение в он-лайне, например "кто-то взломал мой аккаунт". Очень редко приходится обращаться к записям сообщений или чата, когда нарушаются правила виртуального мира. Такое случается, но в исключительных случаях.

9 Научить своих детей не сообщать свой пароль доступа друзьям или родственникам. Это одна из крупнейших проблем, с которой сталкиваются молодые люди на интернет-сайтах. Например, лучший друг или брат/сестра может украсть виртуальные вещи, которые ваш ребенок так упорно коллекционирует.

10 Использовать страницу обратной связи веб-сайта для сообщения о своих опасениях и для того, чтобы задать вопросы. Их работа заключается в том, чтобы вы чувствовали себя удобно на сайте.

11 Не предполагать, что кто-либо в интернете специально преследует вашего ребенка. Статистика показывает, что количество проблем с педофилами в реальном мире намного превышает число онлайновых происшествий. Как правило, детские сайты могут быть безопасными и могут стать великолепным, творческим и социальным опытом для вашего ребенка, но только если вы принимаете участие в его действиях и знаете о них.

Роль, которую могут играть учителя

Очень важно, чтобы учителя не строили догадок о том, что дети и молодые люди могут знать или могут не знать о проблемах электронной безопасности. Существует множество ложных представлений об интернете и о том, что является и что не является приемлемым. Например, многие подростки сообщают друг другу свои пароли и часто считают это проявлением настоящей дружбы.

Важной ролью учителя является сообщить детям и молодым людям о важности паролей, о том, как сделать их безопасными и как создать надежный пароль.

Аналогично, в том, что касается авторских прав, многих взрослых шокирует явное отсутствие беспокойства молодежи относительно фактов скачивания контрафактной музыки и видеороликов. В исследовании[17] предполагается, что, не заботясь об авторских правах, дети и молодые люди совершенно не имеют представления о проблемах законности, связанных с автоскими правами олайнового контента. Опять-таки, очевидно, что задачей учителей является объяснение этого своим ученикам.

В школах имеется возможность изменить программу обучения, с тем чтобы и помочь ученикам полностью использовать свой потенциал, и повысить стандарты образования в области ИКТ.

Однако важно также, чтобы дети узнали, как безопасно использовать эти технологии, в частности такие технологии взаимодействия Web 2.0, как сайты социальных сетей, которые становятся важным аспектом продуктивного и креативного социального обучения. Учителя могут помочь детям использовать технологию разумно и безопасно, следующим образом[18]:

1 Гарантируя, что в школе имеется набор твердых правил и процедур, и их эффективность регулярно оценивается и пересматривается.
2 Гарантируя, что каждый осведомлен о правилах допустимого пользования (AUP) и их применении. Очень важно, чтобы AUP соответствовали возрасту.
3 Проверяя, что школьная политика против запугивания содержит пункты относительно запугивания по интернету и через мобильные телефоны или другие устройства, и что к нарушителям этих правил применяются действенные санкции.
4 Назначив координатора действий по электронной безопасности.
5 Гарантируя, что школьная сеть безопасна и защищена.
6 Гарантируя, что используется лицензированный поставщик услуг интернета.
7 Используя программные продукты фильтрации/мониторинга.
8 Обеспечивая обучение всех детей навыкам электронной безопасности и указывая, где, как и когда это обучение будет проводиться.
9 Гарантируя, что весь персонал, включая обсуживающий персонал, имеет соответствующее образование, и что все регулярно проходят повышение квалификации.
10 Организуя в школе единый пункт для обращений и имея возможность собирать и регистрировать происшествия в области электронной безопасности, что даст возможность школе увидеть лучшую картину в отношении любых проблем и тенденций, которые требуется рассмотреть.
11 Гарантируя, что команда управления и руководители школы имеют достаточно сведений по проблемам электронной безопасности.
12 Проводя регулярную проверку принимаемых мер в области электронной безопасности.

Образовательные и психологические воздействия

В последние годы использование детьми интернет-технологий значительно возросло, и этот рост сопровождается растущей обеспокоенностью относительно проблем онлайновой безопасности. На протяжении истории неоднократно возникала моральная паника по поводу потенциальных опасностей технологий связи,

[17] Berkman Center –John Palfrey and Urs Gasser - 2008

[18] BECTA. Safeguarding Children Online. 2009.

особенно среди молодых женщин. Однако было доказано, что когда такая опасность была изучена, оказалось, что очень часто виновата не технология сама по себе, а то, как дети используют технологию и опасения потерять родительский контроль[19]. Учителя, как ожидается, будут играть жизненно-важную роль в продвижении и обеспечении интернет-безопасности. Оказалось, что родители во всем мире считают, что школа должна играть центральную роль в том, чтобы научить детей безопасному использованию технологий. Коалиция детской благотворительности также предполагает, что "Следует предоставлять школам более понятные рекомендации по безопасному использованию интернета, электронной почты, программ фильтрации и блокировки[20]".

Первые подходы к онлайновой безопасности были сфокусированы, главным образом, на технологических решениях, таких как фильтрующие программы, но в последнее время мы видим растущую мобильность информационных технологий, в результате настольные компьютеры более не являются единственным средством доступа в интернет. В настоящее время, все большее число мобильных телефонов и игровых консолей обеспечивают возможность широкополосной связи, и дети могут входить в интернет, находясь в школе, дома, в библиотеке, в интернет-кафе, в закусочной, в молодежном клубе и даже в транспорте по дороге в школу. Школы предлагают возможность работать в интернете совместно, в рамках закрытой сети или просто в окружении других детей. Очевидные меры включают в себя установку эффективной защиты для сети, но нам необходимо пойти дальше. Дети могут иметь персональные устройства, на которые не распространяется защита сети, и BECTA заявляет, что основной акцент следует сделать на то, чтобы каждый понимал риски и действовал соответственно. Они предполагают, что это означает разработку и реализацию правил электронной безопасности, которые требуют привлечения широкого спектра заинтересованных групп.

Среди них:

1 директора школ;
2 управляющие;
3 старшие менеджеры;
4 классные руководители;
5 обслуживающий персонал;
6 молодые люди, их родители или воспитатели;
7 персонал местных органов власти;
8 поставщики услуг интернета (ISP), поставщики других электронных услуг (ESP), например, владельцы сайтов социальных сетей и региональные консорциумы широкополосной связи, которые работают над мерами обеспечения безопасности сетей в тесном контакте с ISP и ESP.

BECTA уверяет, что поскольку все эти группы имеют свои соображения, которые могут помочь в создании школьных правил, важно, чтобы с ними проконсультировались. Однако, не достаточно просто иметь правила, и каждый, кто занимается детьми, должен использовать активные методы, которые помогают молодым людям и персоналу определить, каким должно быть безопасное поведение, и вести себя соответствующим образом. Поскольку все эти группы привлекаются с самого начала, каждый должен ощущать приемлемость таких правил, а также свою персональную ответственность за соблюдение их в действительности. Создание условий для изучения безопасных ИКТ имеет несколько важных элементов, среди которых следующие:

1 осведомленность о полной инфраструктуре сайта;
2 ответственность, правила и процедуры;
3 эффективный спектр технологических инструментов;
4 всеохватывающее образование в сфере электронной безопасности;

[19] Cassell, J. & Cramer. M. High Tech or High Risk: Moral Panics about Girls Online. In T. McPherson (Ed.) Digital Youth, Innovation, and the Unexpected. The John D. and Catherine T.MacArthur Foundation Series on Digital Media and Learning. Cambridge, MA: The MIT Press, 2008. 53–76.

[20] Children_s Charities_ Coalition for Internet Safety (2001). _Working to make internet a safer place for kids_. Доступен по адресу: www.communicationswhitepaper.gov.uk/pdf/responses/ccc_internet_safety. PDF

5 программа для каждого, кто участвует в создании;

6 процесс пересмотра, в ходе которого непрерывно контролируется эффективность всего вышеописанного[21].

Все это должно быть встроено в существующие правила обеспечения безопасности детей в школе, а не быть чем-то, что команда ИКТ регулирует отдельно. Почти бессмысленно думать, что запугивание по интернету или через мобильный телефон является чем-то иным, чем запугивание в реальном мире. Однако это не означает, что технология также не может быть важной частью решения путем установки:

1 программ предотвращения и защиты от вирусов;

2 систем мониторинга для отслеживания того, кто и что скачивает, когда это было скачано, и какой компьютер использовался;

3 программ фильтрации и контроля контента для сведения к минимуму передачи неподобающего контента по школьной сети.

Очевидно, что проблема, которая возникает в связи с новыми технологиями, относится не ко всем детям, и когда проблемы возникают, они зависят от возраста детей, использующих эти технологии. В конце 2008 года Целевая группа технической безопасности интернета (США) выпустила отчет "Повышение безопасности ребенка и онлайновые технологии", который оказался полезным литературным обзором оригинального опубликованного исследования, касавшегося онлайнового сексуального подстрекательства, онлайнового домогательства и запугивания, а также получения проблематичного контента[22]. В этом отчете отмечается, что "Существует определенное беспокойство в том, что средства массовой информации усиливают эти страхи, и они кажутся намного больше, чем риски, с которыми мы можем столкнуться.

Это создает опасность того, что известные риски будут пропущены, и это понизит вероятность того, что общество учитывает факторы, которые приводят к известным рискам, и часто непреднамеренно вредит молодежи неожиданными способами". Освещение в средствах массовой информации преступлений, совершенных при помощи интернета против детей, часто, как кажется,

[21] BECTA. Safeguarding Дети Online: A Guide for School Leaders: 2009. Available from www.becta.org.uk/schools/safety

[22] ISTTF (2008). Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force To the Multi-State Working Group on Social Networking of State Attorneys General of the United States. Harvard University: The Berkman Center for Internet and Society.

отражает полярные позиции профессионалов и ученых, которые работают в этой области, и маятник качается между теми, кто чувствует опасность искажения угроз, которым могут подвергаться дети, и теми, кому кажется, что угроза сильно недооценивается.

Однако имеется опасение, что интернет-технология может делать некоторых детей уязвимыми и что ответственность за это несет учитель вместе с родителями и опекунами. Мы знаем на удивление мало о том, как дети становятся жертвами, и о факторах, способствующих их умению не поддаваться этому.

Среди форм преследования могут встречаться:

1 Приставание или соблазнение ребенка.
2 Воздействие посредством сомнительных или незаконных материалов.
3 Воздействие посредством среды, которая может оказать тлетворное влияние на поведение части молодых людей.
4 Киберзапугивание.

Удобный способ рассмотрения рисков представлен в таблице[23]:

	Коммерческий	Агрессивный	Сексуальный	Ценности
Контент (ребенок – как получатель)	Реклама Спам Спонсорство Персональная информация	Жестокий/полный ненависти контент	Порнографический или нежелательный сексуальный контент	Дискриминационная, расистская, или вводящая в заблуждение информация или советы
Контакт (ребенок – как участник)	Отслеживание/сбор персональной информации	Запугивание, домогательства или выжидание	Знакомство с незнакомцами или соблазнение	Причинение себе вреда или нежелательные убеждения
Поведение (ребенок – как исполнитель)	Незаконное скачивание, хакерские атаки, азартные игры, финансовое мошенничество или терроризм	Запугивание или домогательства другого человека	Создание и загрузка в интернет неподобающего контента	Предоставление вводящей в заблуждение информации/совета

[23] Таблица разработана проектом EUKids Online и о ней говорилось в параграфе 1.3 обзора компании Byron.

Онлайновое преследование или соблазнение

В контексте сексуального преследования или соблазнения мы больше знаем о процессе обмана, частично потому, что в исследовании участвовало множество детей.

Большая часть результатов этого исследования была получена из Центра исследования преступлений против детей (CCRC) Нью-Хэмпширского университета, а также получено в ходе двух исследований (YISS-1 и YISS-2), которые включали в себя телефонные опросы пользователей интернета страны в соответствии с выборками населения в возрасте от 10 до 17 лет, проведенными в 2000 и 2005 годах. Ссылка на это исследование есть также в Глобальном онлайновом отчете Международного совета по делам молодежи[24, 25]. Кроме того, ссылка на это исследование есть в Глобальном онлайновом отчете Международного совета по делам молодежи[26].

Исследователи недавно предположили, что их работа на тему сексуальных преступлений, инициированных в интернете, ясно показывает, что стереотип интернет-соблазнителя ребенка, который использует обман и насилие для завлечения детей, совершенно не соответствует действительности[27].

Исследование, выполненное в США, полагает, что большая часть преступлений, инициированных в интернете, касались действий взрослого мужчины, использующего интернет для знакомства и склонения к сексуальным отношениям несовершеннолетних подростков.

Интернет-хищники используют такие возможности интернет-общения, как мгновенные сообщения, электронную почту и чат для знакомства и развития интимных отношений со своими жертвами.

В работе показано, что в огромном большинстве случаев жертвы знают о том, что они говорят со взрослыми.

На настоящий момент основной фокус направлен на проблемы детей, которые являются мишенью злонамеренных действий, без должного внимания видам социальных и культурных миров, которые создают в он-лайне молодые люди.

Однако дети и подростки являются не просто мишенями для взрослых в интернете, а активными участниками в создании их собственных киберкультур.

Исследования университета Нью-Хэмпшира подчеркивают, что именно эти аспекты интернета создают риски для некоторых молодых людей, которые вовлечены новыми технологиями в особые способы поведения.

Хотя большинство молодых людей, как выясняется, *идут на риск*, особенно старшие мальчики, все же подавляющее большинство детей *не подвергаются риску*[28].

Однако для молодых людей, которые сообщают незнакомцам персональную информацию, например, имя, номер телефона, фотографии, или разговаривают в он-лайне с такими людьми о сексе, гораздо выше вероятность получения агрессивных сексуальных предложений о контакте или попытке контакта в реальном мире.

В течение пяти лет между YISS-1 и 2 наблюдалось общее уменьшение сексуальных преследований, однако, этого снижения не наблюдалось среди несовершеннолетних и малообеспеченных.

Авторы считают, что такое повышение числа домогательств объясняется, главным образом, ростом

---

[24] Finkelhor, D., Mitchell, K. and Wolak, J. Online victimization: A report on the nation's youth. (NCMEC 6-00-020). Alexandria, VA: National Center for Missing and Exploited Дети. 2000.

[25] Wolak, J. Mitchell, K. and Finkelhor, D. Online victimization: 5 year later (NCMEC 07-06-025). Alexandria, VA: National Center for Missing and Exploited Children. 2006.

[26] http://www.virtualglobaltaskforce.com/iyac_charter_supp.pdf

[27] Wolak, J., Finkelhor, D., Mitchell, K.J., and Ybarra, M.L. Online "predators" and their victims. American Psychologist, 63 (2), 2008 г., 111-128

[28] OPTEM. Safer Internet for Children. Qualitative Study in 29 European Centres. Brussels: European Commission. 2007.

уровня использования интернета за последние пять лет.

Однако в 2005 году вероятность, что молодые люди сообщат об агрессивных преследованиях, была в 1,7 раза больше, даже с учетом изменений демографических характеристик и характеристик использования интернета.

Определенными факторами риска для таких агрессивных преследований, включая преследования со стороны женщин, являются использование комнат чата, мобильного интернета, разговоры с людьми, с которыми впервые познакомились в он-лайне, разглашение персональной информации людям, с которыми впервые познакомились в он-лайне, и подверженность в реальном мире воздействию физического или сексуального насилия.

Во втором обзоре сообщается о 4% (65 случаев) онлайновых просьб передать свою сексуальную фотографию, полученную в течение предшествующего года, но только один молодой человек действительно выполнил такую просьбу.

Факторами риска получения просьбы прислать сексуальную фотографию являются следующие: если это девушка, афроамериканка, если имелись тесные онлайновые отношения, если имело место онлайновое сексуальное поведение и если был опыт сексуального или физического насилия в реальном мире.

Интересен тот факт, что больше вероятности появления таких просьб было, когда молодые люди находились с друзьями и общались со взрослым, которого они впервые встретили в он-лайне, и который отправил сексуальное фото молодому человеку, и пытался или реально осуществил контакт в реальном мире в том или ином виде[29].

В первом обзоре выяснилось, что сексуальные преследования связаны с проявлением признаков депрессии[30].

Молодые люди, которые сообщали о заметных симптомах, напоминающих депрессию, с вероятностью в 3,5 раза большей, сообщали о нежелательном сексуальном преследовании, по сравнению с теми, у кого такие симптомы были слабые или не проявлялись совсем, и те, кто имел такие симптомы в два раза чаще, сообщали об эмоциональном опустошении в связи с инцидентом.

Как правило, опустошение было более обычно для маленьких, которые ощущали агрессивные преследования и для тех, кого преследовали при помощи компьютера вдали от дома[31].

Недавнее исследование в Швеции изучило несколько 16-летних подростков, которые получили приглашения на онлайновую сексуальную встречу и свидания в реальном мире.

Среди 7449 респондентов 46% девочек сообщили, что они получили такие приглашения от взрослых.

Несколько респондентов сообщили о таких преследованиях и в интернете, и по другим каналам.

Соответствующая цифра для мальчиков составила 16%. Подростки получали просьбы раздеться перед веб-камерой или понаблюдать за взрослым, когда тот мастурбирует перед своей веб-камерой.

Подростки, участвующие в исследовании, описывали эти происшествия как обычные, и говорили, что такое случается все время, когда они используют сайты чата.

Ни одна из описанных попыток преследований не была изощренной; взрослый начинал просить о сексуальных услугах с самого начала разговора в чате.

[29] Mitchell, K.J., Finkelhor, D. and Wolak, J. Youth Пользователь интернетаs at risk for the most serious online solicitations. American Journal of Preventive Medicine, 32 (6), 2007, S32-S37.

[30] Ybarra, M.L., Leaf, P.J. and Diener-West, M. Sex differences in youth-reported depressive symptomatology and unwanted Internet sexual solicitation. Journal of Medical Internet Research, 6 (1), 2001, 9-18.

[31] Mitchell, K.J., Finkelhor, D. and Wolak, J. Risk factors for and impact of online sexual solicitation of youth. JAMA, 285 (23), 2001, 3011-3014.

В том же исследовании полиция сообщает о том, что были проанализированы преступления против детей, совершенные при помощи новых технологий, и 50% из них произошли только в он-лайне, причем наиболее частым было поступление просьб передать фотографии или изображения с веб-камеры.

Другими преступлениями, о которых сообщалось, были преступления, совершенные в реальном мире, но в которых первый контакт был осуществлен в интернете.

В половине оффлайновых преступлений жертва познакомилась с интернет-хищником, зная, что их встреча приведет к сексу.

Другие преступления – это были преступления, когда жертва предполагала совершенно другой вид встречи[32].

Недавний подсчет жертв преследований или соблазнений в Швеции и подтверждает, и отвергает результаты Нью-Хэмпширского исследования.

В одном крупном шведском деле, в котором участвовало более 100 девочек, было очевидно, что все девочки знали, что они встречаются с человеком, цель которого – секс с ними.

В то же время ни одна из девочек не признавала, что полностью осознает, что под этим подразумевается.

Что-то в разговорах, которые велись с девочками в чате, давало интернет-хищнику информацию про их уязвимые точки, которые давали ему возможность использовать эти их слабости, даже прежде чем он эксплуатировал их сексуально.

Эти уязвимые точки лежали в диапазоне от одиночества до мыслей о самоубийстве. Тот факт, что девочки на свой страх и риск пошли на встречу с интернет-хищником, не делает их соглашающимися объектами[33].

Очевидно, что число преследований по онлайновым контактам значительно, и что подростки и дети сообщают о том, что это случается, и что все дети знают об этом.

Из рассмотрения случаев, когда происходят преступления как он-лайновые, так и в реальном мире, видно, что просьбы к подросткам, выслать фото или вовлечение в секс с использованием веб-камеры, часто являются признаками начала сексуального домогательства.

В последние годы растет обеспокоенность относительно видов поведения, связанных с сайтами социальных сетей, которое может быть связано с тем, что дети подвергаются риску.

Мы обсудим это дальше, когда будем рассматривать возможности, предоставляемые интернетом молодым людям по вовлечению их в сомнительное поведение, но интересно отметить, что в отчете YISS-2 16% детей сообщали об этом за последний год в своих блогах.

Блоги содержат материал, созданный пользователями интернета и имеют некоторые качества сайтов социальных сетей.

Однако было обнаружено, что подростки и девочки – самые активнее блогеры, а вероятность того, что блогеры будут размещать в он-лайне персональную информацию намного выше, чем для других молодых людей[34].

Однако вероятность того, что блогеры будут общаться с людьми, с которыми он впервые познакомились в он-лайне, но не незнакомы лично, не превышает такой вероятности для обычных молодых людей.

---

[32] Brottsförebyggande Rådet. Vuxnas sexualla kontakter med barn via Internet. [Adults' sexual contacts with Children via the Internet] Report 2007:11. Brottsförebyggande Rådet. 2007. Stockholm.

[33] Wagner, K: Alexandramannen. Förlags AB Weinco. Västra Frölunda. 2008.

[34] Mitchell, K.J., Wolak, J. and Finkelhor, D. Are blogs putting youth at risk for online sexual solicitation or harassment? Chid Abuse and Neglect, 32, 2008, 277-294.

Риск сексуального преследования для блогеров, которые не взаимодействуют, не более высок, и размещение в сети персональной информации не повышает этого риска.

Однако блогеры подвергаются более высокому риску домогательств в реальном мире, вне зависимости от того, взаимодействуют ли они с другими людьми в он-лайне.

В обзоре UK Children Go Online предполагается также, что молодые люди, которые менее всего удовлетворены своей жизнью и которые часто и квалифицированно используют интернет, по всей видимости, будут более высоко ценить интернет как среду общения, что может привести к более рискованным действиям[35].

Из известных случаев и в результате опыта можно выделить несколько факторов, которые необходимо изменить, если мы собираемся помочь тем детям, которых склоняют в он-лайне к сексуальному насилию в реальном мире.

Мы узнали, что онлайновое соблазнение в отличие от офлайнового происходит быстрее и может быть анонимным: дети быстрее начинают доверять своим онлайновому "другу" и становятся менее замкнутыми, в том как они общаются, и таким образом интернет-хищники не ограничены во времени или доступности, как это было бы в реальном мире.

Как правило, интернет-хищники узнают все, что могут, о своей потенциальной жертве; определяют риск и вероятность того, что ребенок рассказывает, узнают о круге его общения; могут сообщить ложную информацию о себе, включая фальшивые фотографии, и, если все достаточно безопасно, они начинают устанавливать "отношения" с ребенком или управлять ребенком так, чтобы организовать встречу с ребенком в реальном мире[36].

Терапевтические сеансы, помогающие детям и подросткам, ставшими жертвами в реальном мире и подвергавшихся онлайновой эксплуатации, в настоящее время расследуются в BUP Elefanten, который является психиатрическим отделением для детей и подростков, которое работает с детьми, подвергшимися сексуальному или физическому насилию в Швеции.

Этот проект выполняется с 2006 года, терапевтами, полицией, прокурорами и социальными работниками, было проведено более 100 интервью с молодыми людьми.

Эти молодые люди были объектами различных домогательств, включая сексуальное домогательство, участие в сексе перед вебкамерой; загрузки фотографий в интернет; онлайновое вовлечение, ведущее к насилию в реальном мире, и продажа детского секса в онлайновом режиме[37].

Анализ данных этих интервью предполагает, что этих молодых людей можно разделить на три группы:

1. те, кого обманули и кого мошенническим образом вовлекли во что-то неожиданное для них;
2. те, кто рискует для удовлетворения эмоциональных потребностей и привлечения внимания;
3. и саморазрушители, которые, например, продают секс или сознательно вступают в опасные отношения.

[35] Livingstone, S. and Helsper, E.J. Taking risks when communicating on интернет. The role of offline social-psychological factors in young people's vulnerability to online risks. Information, Communication and Society, 10 (5), 2007, 618-643.

[36] Palmer, T. Just One Click. London: Barnardos. 2004.

[37] Quayle, E., Lööf, L. & Palmer, T. (2008). Child Pornography And Sexual Exploitation Детей Online. Bangkok: ECPAT International

Последняя группа, как правило, не хочет видеть себя жертвами, вместо этого они считают, что у них все под контролем.

Результаты этих клинических исследований позволяют предположить, что многие из этих детей отклоняют предложения помощи, и важно, что врачи не сдаются, работая с этими детьми, а наоборот стараются поддерживать контакт с ними до тех пор, пока они не почувствуют их готовность принять помощь или разрешить вмешательство.

Один из главнейших факторов воздействия процесса соблазнения на детей, которые являются субъектами злонамеренных изображений, приводит к тому, что дети молчат.

Это молчание вызвано тем фактом, что молодые люди на самом деле верят в то, что человек, с которым они собираются познакомиться, является их другом и что они не будут безропотно подчиняться тому характеру разговора, который они вели в онлайновом режиме.

Первый пункт имеет косвенное указание на то, как молодые люди определяют дружбу, последний пункт связан с тем фактом, что, как упомянуто выше, молодые люди испытывают меньшие опасения при общении в режиме он-лайн.


“Интернет может перенести детей и молодых людей практически в любое место мира – и в течение этого процесса они могут подвергаться потенциально опасным рискам”

Доступ к сомнительным материалам

Хотя было бы наивно предполагать, что порнографических или сексуальных материалов до интернета не существовало вообще, правда заключается в том, что интернет принес с собой быстрое распространение легкодоступных сексуальных материалов.

Доступность, интерактивность и анонимность интернета, однако, являются теми самыми факторами, которые повышают вероятность подверженности воздействию жестоких или сексуальных материалов.

В исследовании SAFT 34% детей увидели веб-сайт с жестокими материалами либо случайно, либо осознанно[38].

Нью-Хэмпширское исследование подчеркнуло наличие возможности случайного влияния на людей нежелательного сексуального материала в интернете, но оно также признало тот факт, что существующее исследование, изучающее влияние такого воздействия нежелательного сексуального материала, проведено, главным образом, среди студентов и молодых взрослых, а не среди маленьких детей, и касалось, главным образом, добровольного, а не случайного воздействия.

Предполагается, что различные типы подростков, вовлеченных в злонамеренные или эксплуативные отношения в онлайновом режиме, могут показать, что любители риска и молодые люди, склонные к саморазрушению, могут также просматривать порнографию или посещать сайты с чатами, тем самым оказывая услуги взрослым, ищущим партнеров для секса, по этому поводу исследований было недостаточно.

В исследовании YISS-1 показано, что в течение года до сбора данных 1 из 4 детей, регулярно использующих интернет, встречал нежелательные сексуальные изображения. 73% таких случаев происходит, когда молодой человек использует интернет, и большая их часть происходит, когда он дома, а не в школе.

Авторы обзора также обсуждают способы, которыми программные средства, обеспечивающие такое воздействие, затрудняют возможность избежать встречи с ними. Такие "мышеловки" устроены в одной трети таких возмутительных инцидентов.

Большинство детей, испытавших воздействие материала, не считают такое воздействие особенно опасным.

Однако авторы подчеркивают, что такое воздействие, особенно нежелательное воздействие, может повлиять на отношение к сексу, интернету, и чувство безопасности и общности молодых людей.

В исследовании YISS-2 отмечен рост числа случаев нежелательного воздействия порнографии, и особенно заметно оно было среди детей в возрасте 10–12 лет, и старших мальчиков 16–17 лет – белых и не из Латинской Америки[39].

В исследовании австралийской молодежи (16-, 17-летних) три четверти случайно подвергались воздействию порнографических веб-сайтов, при этом 38% мальчиков и 2% девочек специально выходили на такие сайты[40].

Это исследование пришло к выводу, что два параметра воздействия детских порнографических веб-сайтов отражают функции взрослых сайтов.

---

38 SAFT. Safety Awareness Facts Tools. Brussels: European Commission. Accessed 5.6.2007 from: http://ec.europa.eu/information_society/activities/sip/projects/awareness/closed_projects/saft/index_en.htm.

39 Mitchell, K.J., Wolak, J. and Finkelhor, D. Trends in youth reports of sexual solicitations, harassment, and unwanted exposure to pornography on интернет. Journal of Adolescent Health, 40, 2007, 116-126.

40 Flood, M. Exposure to pornography among youth in Australia. Journal of Sociology, 43 (1), 2007, 45-60.

Во-первых, мальчики более вероятно ищут порнографические фильмы и сайты, и являются их более частыми потребителями.

Во-вторых, пользователи интернета любого возраста считают трудным избежать нежелательных встреч с сексуальными материалами.

Пример этого связан с некоторыми компьютерными играми, которые могут нести значительную сексуальную компоненту.

Такие игры могут считаться играми "для взрослых", но они неизменно пользуются успехом у большого числа молодых людей.

Важно отметить также, что такое воздействие не является уникальным результатом новых технологий, но они существуют и в более традиционных средствах информации – телевидении, где часы вещания эротических и сексуальных материалов могут приходиться на время, когда со всей вероятностью могут увидеть дети.

Фактор, который может иметь значение здесь, относится к контролируемости воздействия, и здесь можно различить влияние случайного и осознанного воздействия.

Было также обнаружено, что есть множество маленьких детей, которых удивляет содержание материала, который они несознательно встречают, пользуясь интернетом [41].

Неожиданный или частичный доступ к материалу может быть важной проблемой, и предполагалось, что[42]: "Новейшие технологии, включая видео, интернет и мобильную связь, позволяют увидеть контент вне контекста.

Кто-то может увидеть набор роликов, а не целую историю, по которой можно понять контент. Редактирующий контекст всегда важен в контенте указаний по регулированию (например BBFC, Ofcom), что может быть трудно встроить в параллельные указания для новых средств информации.

Однако из исследования ясно, что случайное воздействие на детей порнографии в интернете, которая является неожиданным и не соответствующим обстановке контентом, может быть особенно раздражающим. Это ставит перед регуляторами сложные задачи".

Однако использование порнографии молодыми людьми еще не было исследовано достаточно хорошо, и результаты строятся, главным образом, на разрозненных самоотчетах, разница в которых вполне может быть такой, которую превалирующие социальные нормы диктуют для действий подростка.

Можно предположить, что многие дети и подростки заявят, что они наткнулись на порнографию случайно, поскольку считается нецелесообразным утверждать, что они активно искали ее в интернете.

В шведском примере 18-летних 65% мальчиков смотрели порнографию ежемесячно, а среди девочек таких было только 5%. Следует отметить, что только 7% мальчиков и 31% девочек в исследовании заявили, что они никогда не видели порнографии[43].

[41] Fug, O.C. Save the дети: The protection of minors in the information society and the audiovisual media services directorate. Journal of Consumer Policy, 31, 2008 г., 45-61.

[42] Livingstone, S. and Hargrave, A.M. Harmful to дети? Drawing conclusions from empirical research on media effects. In U. Carlsson (ed) Regulation, Awareness, Empowerment. Young people and Harmful Media Content in the Digital Age. Göttenborg: Nordicom. 2006.

[43] Mossige, S., Ainsaar, M. and Svedin, C.G. The Baltic Sea Regional Study on Adolescent´s Sexuality. NOVA Rapport 18/07. Oslo: NOVA, s. 93-111

Многие молодые люди подвергались онлайновому влиянию сексуальных материалов, и мы явно видим, что не все это воздействие является случайным и разрушительным.

Одно из опасений состоит в том, какое воздействие аномальная и жестокая порнография может оказать на взгляды и восприятие мира некоторых молодых людей и, в меньшей степени, на поведение лишь небольшого числа.

Это все чаще рассматривается, как потенциальная проблема для здоровья населения, и может показаться, что последствия воздействия в большой и нерегулируемой среде, то есть в интернете, определенно требуют дальнейшего изучения[44].

Сомнительные возможности

Одна их дополнительных опасностей со стороны новых технологий связана с самими средствами информации и возможностями, которые позволяют молодым людям, оказаться вовлеченными такими способами, которые могут вызывать глубокое беспокойство.

Это можно назвать действиями по самовиктимизации как посредством технологий интернета, так и через мобильный телефон, хотя этот термин может показаться сомнительным, поскольку он сильно связан с повышением возможностей создания онлайнового контента.

Факты говорят, что у детей возраста 11–16 лет мобильных телефонов, больше, чем у взрослых, 76%детей имеют собственный телефон[45].

[44] Perrin, P.C., Madanat, H.N., Barnes, M.D., Corolan, A., Clark, R.B., Ivins, N. et al. Health educationa's role in framing pornography as a public health issue: local and national strategies with international implications. Promotion and Education, 15, 2008 r., 11-18.

[45] Child-Wise Monitor (2002). Accessed on 18.06.07 at: http://www.childwise.co.uk/monitor.htm

Обзор 1340 учеников средней школы из области Тисайд Соединенного Королевства, проведенный в 2004 году, показал, что 86% из них имели мобильный телефон (89,7% девочек и 82,3% мальчиков)[46].

В этом исследовании использование мобильного телефона было ограничено только голосовой связью и передачей текста, но есть свидетельства того, что мобильные телефоны все больше используются как другие виды связи.

Однако в исследовании "*Дети в онлайне*" в Соединенном Королевстве показано, что теперь все диверсифицируется, и 38% молодых людей имеет мобильный телефон, 17% – цифровой телевизор и 8% – игровую консоль, все – с выходом в интернет.

Для многих молодых людей мобильный телефон является и жизненно важным средством общения, и способом принадлежности и участия в расширенном социальном мире.

Количественное исследование OPTEM 2007 года, охватывавшее 29 европейских стран, показало, что подавляющее большинство детей имеет мобильные телефоны.

Однако появляются беспокойства, что такое увлечение технологическим участием может подразумевать действия, которые нацелены на других людей или вовлекают самих молодых людей.

Созданные самими пользователями изображения или фильмы можно считать частью процесса соблазнения, в котором интернет-хищник убеждает ребенка переслать ему свои изображения либо без одежды, либо в процессе выполнения сексуальных действий.

Изображения часто используются для убеждения ребенка в безопасности сексуальных контактов между ребенком и взрослым, уменьшая у ребенка ощущение запретности участия в реальных сексуальных действиях или в получении платы от взрослого за встречу.

Дети, на которых направлены эти действия, являются уязвимыми по многим причинам, например, они одиноки, запуганы или постоянно ссорятся со своими родителями. Вовлеченный подросток после отправки изображений интернет-хищнику, ощущает себя соучастником преступления.

Вопрос ущерба также изучался группой Нью-Хэмпширского университета посредством рассмотрения историй пациентов 1504 врачей, с тем чтобы увидеть, о каких типах сомнительного опыта сообщалось как о связанных с новыми технологиями.

Было определено одиннадцать типов сомнительного опыта, о которых сообщали как молодые, так и взрослые клиенты.

Это было: злоупотребление; порнография; неверность; сексуальная эксплуатация; насилие; игры; азартные и ролевые игры; домогательства; не зависящее от окружения и неконтактное использование; мошенничество, воровство и жульничество; несложившиеся онлайновые взаимоотношения; вредное влияние веб-сайтов, а также рискованное и неподходящее использование[47].

Дальнейший анализ рассматривает, какие виды сомнительного опыта были определены как основные и какие как вторичные проблемы[48].

Более вероятно, что молодые и взрослые пользователи будут иметь проблемы, связанные со злоупотреблением интернета, использованием взрослой порнографии, детской порнографии, преступлениями в сфере сексуальной эксплуатации, играми, азартными и ролевыми играми.

[46] Madell, D. and Muncer, S. Back from the beach but hanging on the telephone? English adolescents' attitudes and experiences of mobile phones and Internet. CyberPsychology and Behavior, 7 (3). 2004, 359-367.

[47] Mitchell, K.J., Becker-Blease, K.A. and Finkelhor, D. Inventory of problematic Internet experiences encountered in clinical practice. Professional Psychology: Research and Practice, 36 (5), 2005, 498-409.

[48] Mitchell, K.J. and Wells, M. Problematic Internet experiences: Primary or secondary presenting problems in persons seeking mental health care? Social Science and Medicine, 65, 2007, 1136-1141.

Другие проблемы, связанные с интернетом, такие как зависящее от окружения и неконтактное использование, роль жертвы в сфере сексуальной эксплуатации, преступлениями в сфере домогательств, онлайновая неверность – равновероятны.

Проблемы молодых людей, связанные с играми, азартными играми и ролевыми играми, с вероятностью в 1,7 раз большей, определяются как основные проблемы, а онлайновое мошенничество или жульничество – вероятностью в четыре раза больше.

Молодым людям, являющимся жертвами сексуальной эксплуатации, более вероятно поставят диагноз посттравматического стрессового расстройства (PTSD), чем молодым людям с другими связанными с интернетом проблемами.

Запугивание

Мы уже отмечали, что не следует считать запугивание в онлайновом мире чем-то отличным от того, что мы видим в реальном мире.

Люди иногда называют онлайновое запугивание или запугивание по мобильному телефону "киберзапугиванием", но это никому не помогает понять, что происходит. Запугивание остается запугиванием, вне зависимости от того, где и как оно происходит.

В исследовании компании Byron, выполненном в Соединенном Королевстве, предполагается, что "Киберзапугиванием называется запугивание, которое осуществляется при помощи электронных средств связи, например, путем отправки текстовых сообщений с угрозами, размещение в сети неприятных сведений о людях и распространение неприятных фотографий или видеороликов о ком-либо".

Онлайновое запугивание или запугивание по мобильному телефону может быть продолжением личного запугивания, или может быть формой продолжения событий, происходящих в реальном мире. Онлайновое запугивание или запугивание по мобильному телефону может быть особенно неприятным или разрушитель-

ным, так как оно распространяется в более широких масштабах, с большей степенью публичности, и распространяемый в электронном виде контент может в любое время снова всплыть на поверхность, что еще более усложняет ситуацию для жертвы запугивания, затрудняет завершение инцидента; он может содержать дискредитирующие визуальные изображения или оскорбительные слова, содержание доступно 24 часа в сутки; запугивание при помощи электронных средств связи может происходить 24 часа в сутки, 7 дней в неделю, то есть оно может вторгаться в частную жизнь жертвы даже в тех местах, которые в ином случае являются "безопасными", даже дома; и персональная информация может быть искажена, фотографии изменены и затем переданы другим людям. Более того, оно может быть осуществлено анонимно[49]".

Такие действия по запугиванию могут состоять как из попыток подначивания, так и из очень агрессивных действий, и исследования Университета Нью-Хэмпшира делают вывод, что существует значительное перекрытие между незаконными действиями, такими как сексуальные домогательства, и запугиванием.

Недавние исследования в Германии рассматривали возможных жертв запугивания в чатах интернета[50].

Они определили различные типы запугивания, среди которых домогательство, ругательство, оскорбление, подначивание и шантаж.

Такое запугивание наблюдалось часто, и зачастую оно было нацелено на одних и тех же детей.

Важно, что эти исследования показали наличие связи между преследованиями в школе и в чатах интернета.

Вероятность преследования в чатах интернета выше для тех подростков, которых запугивают в школе.

Более вероятно, что такие дети менее популярны и имеют более низкую самооценку и гиперопекающих родителей.

В этом исследовании также предполагается, что эти дети могут переходить из жертв в преследователей, и эти перемещения можно считать "ответом ударом на удар" или "выпусканием пара".

Жертвы запугивания в чатах интернета, как сообщается, часто посещают рискованные онлайновые локации и в действительности оказываются в ситуациях, где вероятность преследования выше.

В исследовании указано, что по сравнению с большинством жертв запугивания в школе, большинство жертв запугивания в чате чаще проявляют манипуляционное поведение, посещая чаты, например, дают неверную информацию о своем возрасте или половой принадлежности.

Исследование в отношении американских детей привело к выводу, что:

1 для заядлых пользователей интернета "киберзапугивание" является обычным делом;

2 формы онлайнового и школьного запугивания очень похожи, и ситуации этих двух вариантов пересекаются;

3 хотя некоторые электронные средства и устройства связи связаны с увеличением риска "киберсзапугивания", они – всего лишь инструменты, а не причина неприглядного поведения;

4 киберзапугивание, которое никак не связано с запугиванием в школе, связано с повышенным стрессом;

5 молодые люди редко говорят взрослым о происшествиях онлайнового запугивания и не могут полностью использовать инструменты, предоставляемые технологиями связи для предотвращения таких инцидентов в будущем[51].

[49] Byron, T. (2008). Safer Дети in a Digital World The Report of the Byron Review. Available from http://www.dcsf.gov.uk/byronreview/pdfs/Final%20Report%20Bookmarked.pdf

[50] Katzer, C., Fetchenhauer,D. and Belschak, F. Cyberbullying: Who Are the Victims? A Comparison of Victimization in Internet Chatrooms and Victimization in School. Journal of Media Psychology 2009; Vol. 21(1):25–36.

[51] JUVONEN, J. & Gross, G.F. Extending the School Grounds?—Bullying Experiences in Cyberspace. Journal of School Health, 2008 г., 78 (9), 496 – 505.

4. Руководящие указания для родителей, опекунов и учителей

Полезные советы по поводу личной безопасности основываются на анализе собранных данных и результатах имеющихся исследований. Этот раздел документа предназначен, для того чтобы собрать в одном удобном месте рекомендации для родителей, опекунов и учителей с целью помочь им научить своих детей тому, как оставаться в безопасности, и получить положительный и ценный опыт, находясь в онлайновом режиме.

Родители, опекуны и учителя до принятия решения о том, какие условия пригодны для их ребенка, должны учесть настоящий характер различных сайтов, степень понимания их детьми опасностей и вероятность того, что родители могут уменьшить риски.

Интернет имеет огромный потенциал как средство дать детям и молодым людям возможность отыскания нужных им вещей. Ключевой задачей является научить их вести себя в он-лайне позитивно и ответственно.

Родители, опекуны и учителя			
	№	Основные аспекты, требующие внимания	Описание
Защита и безопасность вашего персонального компьютера	1	Поставьте компьютер в общей комнате	Размещение компьютера в общей комнате и присутствие в ней, особенно, когда интернетом пользуются маленькие дети, может быть очень важным. Если вы не можете присутствовать, рассмотрите другие способы внимательного наблюдения за тем, что делают дети в он-лайне, например, используя технические инструменты. В больших семьях с несколькими компьютерами, могут существовать некоторые ограничения, которые также усиливаются, если вы настаиваете на том, чтобы все компьютеры были в одной и той же комнате в одно и то же время, только помните, что, становясь старше, дети все равно получат некоторую самостоятельность. С ростом числа детей, имеющих лэптопы, и с учетом того, что беспроводные сети становятся обычным явлением в частных домах, соблюдать правила такого рода будет все сложнее.
	2	Установите брэндмауэр и антивирусное программное обеспечение	Удостоверьтесь, что на вашем компьютере установлен брэндмауэр и антивирусное программное обеспечение, и что оно обновлено. Научите ваших детей основам интернет-безопасности.
Правила	3	Договоритесь о правилах использования дома интернета и персональных устройств, обращая особое внимание на секретность, места, несоответствующие возрасту, запугивание и опасность незнакомцев	Как только дети начинают пользоваться интернетом самостоятельно, обсудите с ними и создайте список согласованных правил. Эти правила должны определять, когда дети пользуются интернетом и как они им пользуются.
	4	Договоритесь о правилах использования мобильного интернета	Как только дети начинают пользоваться мобильным телефоном, обсудите с ними и создайте список согласованных правил. Эти правила должны определять, имеют ли дети право выходить в интернет через мобильный телефон, и как часто они могут использовать его, какие виды материалов они могут покупать или скачивать, используя его, как обращаться с неприемлемыми предметами, и уровни затрат.

Родители, опекуны и учителя			
	№	**Основные аспекты, требующие внимания**	**Описание**
Обучение родителей, опекунов и учителей	5	Родители должны познакомиться с интернет-сайтами, используемыми их детьми, т. е. услугами и продуктами, предлагаемыми интернет-сайтами, и хорошо понимать, как дети проводят время в он-лайне	Оцените сайты, которые дети собираются использовать, и внимательно прочтите их политику конфиденциальности, правила использования и правила поведения, которые часто называются "правилами внутреннего распорядка", а также все страницы для родителей. Кроме того, узнайте, проверяет ли сайт размещаемый на нем контент или служебные страницы, и периодически просматривайте страницу вашего ребенка. Проверьте, какие продукты продаются на сайте, если таковые есть.
	6	Изучайте онлайновые ресурсы, чтобы получить дополнительную информацию об онлайновой безопасности и о том, как безопасно использовать интернет	Приятное и безопасное использование интернета празднуется по всему миру ежегодно. В таком празднике могут участвовать дети, местная школа, промышленность и соответствующие участники рынка, сотрудничающие в деле создания большей осведомленности о возможностях продвижения положительного опыта в онлайновых действиях. Самую свежую информацию о таких событиях можно найти в поисковых машинах, используя поиск с запросами типа "празднование безопасного использования интернета" + "название страны".
	7	Имейте представление о том, как дети используют другие персональные устройства, такие как мобильные телефоны, игровые консоли, MP3-плееры и PDA	Сегодня доступ в интернет можно получить при помощи нескольких разных персональных устройств, поэтому в этих условиях возникают аналогичные проблемы безопасности.

	№	Основные аспекты, требующие внимания	Описание
Обзор возможностей интернет-сайтов	8	Учитывайте, как программы фильтрации и блокировки или мониторинга могу помочь или поддержать безопасность использования интернета и персональных устройств детьми и молодыми людьми. Если вы используете такие программы, объясните своим детям, как они работают и почему вы их используете. Храните в секрете любые пароли, связанные с этими программами	При использовании технических средств могут возникать проблемы доверия и прав молодого человека на конфиденциальность, особенно при использовании программ мониторинга. В обычных условиях очень желательно, чтобы родитель или опекун объяснил причины, по которым он хочет использовать этот тип программ, и ее использование школе также должно быть объяснено.
	9	Согласие родителей	В некоторых странах, например в Испании и США, имеются законы, определяющие минимальный возраст, до которого компания или веб-сайт обязаны просить молодого человека представить персональную информацию о себе без получения проверяемого согласия родителей. В Испании это – 14 лет, в США – 13. В других странах считается хорошим тоном потребовать согласия родителей, прежде чем спрашивать молодого человека о его персональных данных. Многие сайты, предназначенные для маленьких детей, должны спрашивать согласия родителей, прежде чем разрешить новому пользователю зарегистрироваться на сайте. Проверьте, какие требования относительно согласия родителей имеются на сайтах, где хотят зарегистрироваться ваши дети или где они уже зарегистрированы.
	10	Контролируйте использование кредитных карт и других платежных механизмов	Контролируйте использование фиксированных или мобильных телефонов для покупки виртуальных товаров. Соблазн может быть слишком большим, когда детям разрешают использовать фиксированные или сотовые телефоны для покупки каких-либо видов товаров и услуг. Также храните свои кредитные и дебетные карты в безопасности и не разглашайте свои пин-коды.

	№	Основные аспекты, требующие внимания	Описание
	11	Удостоверьтесь в том, что при онлайновой продаже товаров и услуг используется проверка возраста	Обычно при покупке товаров возраст не проверяется, однако системы все чаще имеют возможность проверить возраст в точке продажи. Во всех случаях внимательно наблюдайте за тем, что делает ваш ребенок в он-лайне.
	12	Проверьте, используется ли модерация на интернет-сайте	Удостоверьтесь в том, что на интернет-сайте есть модерация разговоров: в идеале, и автоматические средства используются, и человек-модератор контролирует разговоры. Просматривает ли сайт все фотографии и видеоролики, которые на нем размещаются?
	13	Блокируйте доступ к нежелательному контенту или услугам	Технические средства могут помочь вам заблокировать доступ к нежелательным веб-сайтам, например, к тем, которые допускают немодерируемый контент или обсуждения, либо заблокировать доступ к нежелательным услугам или контенту на мобильные телефоны.
	14	Проверьте гибкость регистрации	Проверьте, как можно удалить аккаунт – даже если это приведет к потере уплаченной абонентской платы. Если услуги не позволяют удалить аккаунт, рассмотрите возможность отказаться от его использования или заблокировать доступ к нему. Сообщайте местным властям о невозможности удалить аккаунт.
	15	Просмотрите описание предоставляемых услуг	Проанализируйте правила поставщика контента и их соблюдение, просмотрите контент и конкретные предоставляемые услуги, и узнайте о технических ограничениях, например, реклама не всегда отмечена как реклама.
	16	Наблюдайте за рекламой и сообщайте о неподходящей рекламе	Наблюдайте за рекламой и сообщайте в местный совет по рекламе о: 1 Введении в заблуждение за счет чрезмерного упрощения сложных проблем. 2 Вовлечении детей в разговоры с незнакомцами или приглашении их в опасные места. 3 Демонстрации людей и, особенно, детей, использующих опасные вещи, или находящихся поблизости от опасных вещей. 4 Поощрении небезопасного моделирования опасных действий. 5 Поощрении запугивания. 6 Причинении морального ущерба и запугивание детей. 7 Поощрении плохих привычек питания. 8 Эксплуатации детской доверчивости.

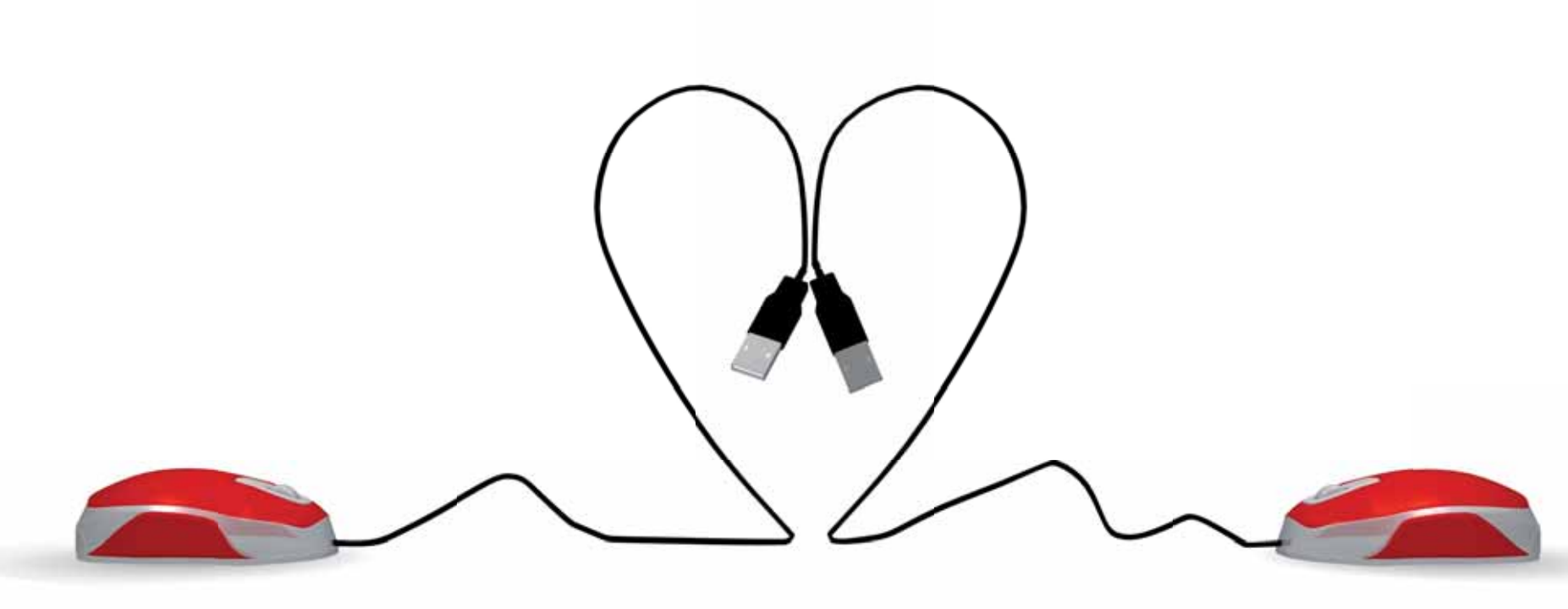
	№	Основные аспекты, требующие внимания	Описание
Обучение детей	17	Обучайте своих детей	Образование и компьютерная грамотность очень важны. Объясните детям рекомендации и правила виртуальных миров. Дети, по всей видимости, примут рекомендации и будут напоминать другим делать то же самое. Научите своих детей не отвечать на грубые сообщения и избегать разговоров о сексе в он-лайне Научите их не открывать прикрепленные файлы или ссылки, которые они получают от других лиц во время разговора в чате, потому что они могут содержать вредный контент.
	18	Объяснить детям, что нельзя договариваться о личной встрече с человеком, с которым они впервые познакомились в он-лайне	Дети могут подвергаться реальной опасности, если они будут лично встречаться с незнакомцами, с кем общались только в он-лайне. Родителям следует убеждать своих детей использовать интернет-сайты для общения только со своими реальными друзьями, а не с людьми, которых они никогда не видели. Люди в он-лайне могут быть совсем не теми, за кого себя выдают. Однако если сформировалась крепкая онлайновая дружба, и ваш ребенок желает устроить встречу, то не подвергайте его риску, отпуская одного или без сопровождения, ясно скажите ему, что собираетесь пойти вместе с ним, или удостоверьтесь, что с ним пойдет другой взрослый, которому вы доверяете, и убедитесь, что первая встреча назначена в общественном месте, что оно хорошо освещено и вокруг много людей.
	19	Предупреждайте детей о недопустимости разглашения персональной идентификационной информации	Помогите своим детям понять, какую информацию следует хранить в секрете. Объясните детям, что им следует давать только ту информацию, которую, по вашему и его мнению, допустимо увидеть посторонним. Напоминайте вашим детям, что однажды передав информацию в интернет, они не смогут забрать ее обратно.
	20	Убедитесь, что дети понимают, что значит – выложить фотографию в интернет, включая использование веб-камер	Объясните детям, что фотография может раскрывать массу личной информации. Детям не следует разрешать пользоваться веб-камерами или загружать в интернет какой-либо контент без согласия родителей или ответственного взрослого. Не разрешайте детям самостоятельно загружать фотографии себя или своих друзей с ясно определяемыми подробностями, например, табличками с названиям улиц, номерными знаками автомобилей или названием школы на свитерах.

	№	Основные аспекты, требующие внимания	Описание
	21	Предупреждайте детей насчет выражения чувств в присутствии незнакомцев	Детям не следует напрямую общаться с незнакомцами в он-лайне. Объясните детям, что все, что они пишут, может прочесть кто угодно, у кого есть доступ к этому сайту, и что интернет-хищники и хулиганы часто ищут детей, которые заинтересованы в нахождении новых друзей в он-лайне.
Обзор безопасного использования интернет-сайтов	22	Проверьте страницу и профиль вашего ребенка	Регулярно проверяйте страницу вашего ребенка. Войдите с паролем, чтобы посмотреть историю аккаунта вашего ребенка и, при необходимости, измените режим общения в чате до уровня, который вам кажется приемлемым. Правильно сделанные интернет-сайты предоставляют вам возможность быть полностью осведомленным о времяпрепровождении вашего ребенка. Если ребенок отказывается выполнять правила сайта, вы можете попробовать связаться с сайтом, попросить удалить страничку и профиль вашего ребенка. Помимо прочего, эти действия должны подкрепить ваши слова относительно важности правил и о последствиях их нарушения.
	23	Удостоверьтесь в том, что дети соблюдают ограничения интернет-сайта	Если дети еще не доросли до возраста, рекомендованного интернет-сайтами, не позволяйте им пользоваться ими. Важно помнить, что родители не могут полагаться на то, что поставщик услуг сумеет не разрешить ребенку зарегистрироваться.
	24	Удостоверьтесь в том, что дети не используют полные имена	Везде, где возможно, пусть дети используют ник, а не свое имя или его часть. Ник следует выбирать осторожно, так чтобы он не привлекал ненужного внимания. Не позволяйте детям сообщать полные имена своих друзей или любую другую информацию, которая может использоваться для их идентификации, например, название улицы, на которой они живут, по которой они ходят в школу, их номера телефонов, спортивные клубы и т. д.

Учителя[52]			
	№	Основные аспекты, требующие внимания	Описание
Общение	25	Обсуждайте с детьми полученный ими опыт	Регулярно беседуйте с детьми о том, на какие сайты они ходят и с кем они разговаривают, когда находятся в он-лайне. Поощряйте рассказы детей, если они встретили в интернете что-то, что заставило их почувствовать неудобство или испуг. Напомните детям, что надо сразу же прекратить делать что бы то ни было, как только они почувствуют неудобство или заподозрят что-нибудь. Удостоверьтесь, что они не попадут в неприятности, когда привлекают к чему-то ваше внимание. В свою очередь, вы как родитель и взрослый, не должны слишком остро реагировать, когда ребенок делится с вами впечатлениями. Оставайтесь спокойными вне зависимости от того, что они вам говорят, узнайте все факты и затем действуйте. Похвалите ребенка за то, что он вам рассказал. Удостоверьтесь, что дети могут сообщить об обидчиках.
Безопасность и защищенность как часть стратегии защиты ребенка	1	Используйте полноценный подход к ответственности за электронную безопасность	Важно, чтобы даже если школа не позволяет применять в стенах школы определенную технологию, учителя научили учеников, как разумно и ответственно вести себя при ее использовании, и рассказали о рисках.
	2	Разработайте правила допустимого использования (AUP)	В них должны быть подробно описаны способы, а также то, как персонал, ученики и все пользователи сети, включая родителей, могут и как не могут использовать средства ИКТ.
Принципы и правила	3	Примеры различных AUP можно найти как в интернете, так и через местные органы власти	Важно доработать эти правила так, чтобы они соответствовали конкретной ситуации учебного заведения.
	4	Сопоставьте AUP с правилами других школ	Они должны содержать такие правила, как антизапугивание и рекомендации по авторским правам и плагиату.
	5	Единый координатор	Назначьте одного из старших руководителей, ответственного за обеспечение безопасности, также главным координатором по всем проблемам электронной безопасности.

[52] BECTA (2008) Safeguarding children online. A guide for school leaders. Доступен по адресу:: www.becta.org.uk/schools/safety

	№	Основные аспекты, требующие внимания	Описание
	6	Потребность в руководстве	Директора школ при поддержке властей должны руководить введением в действие согласованных правил электронной безопасности.
	7	Поддерживайте осведомленность среди молодых людей	Удостоверьтесь, что молодые люди, за которых вы отвечаете, осведомлены о возможных рисках и о том, как вести себя безопасно и ответственно всегда и везде, когда они в он-лайне.
	8	Поддерживайте способность к защите	Позволяйте молодым людям разрабатывать собственные стратегии защиты на те случаи, когда рядом нет взрослого и не доступны технические средства защиты.
	9	Поощряйте раскрытие угроз и принятие ответственности	Помогите молодым людям понять, что они не отвечают за действия, которые другие люди могут выполнять в отношении них, но что существуют меры, которые предпримет школа, если они ведут себя в он-лайне неподобающим образом.
Технологиче-ские решения	10	Методы аудита	Удостоверьтесь в том, что технологические меры и решения регулярно проверяются и обновляются для обеспечения эффективной работы программы электронной безопасности
Правила безопасности интернета	11	Обучите учителей правилам безопасности интернета	Обучите учителей правилам безопасности интернета, для того чтобы они могли помочь детям оставаться в безопасности, выходя в сеть.
	12	Научите студентов никогда не разглашать персональную информацию, общаясь с другими людьми	Сообщите студентам, что персональная информация, например, полное имя, адрес, адрес электронной почты, номер телефона, название школы и т. д. никогда не следует разглашать, общаясь с незнакомцами в он-лайне.
	13	Требуйте, чтобы студенты искали в сети только конкретную информацию	Требуйте, чтобы студенты искали в сети конкретную информацию, а не "лазили" по интернету наобум и затем записывали в библиографическом формате URL используемые ими сайты.
	14	Просматривайте тексты веб-сайтов, прежде чем дать ссылки на них студентам	Обязательно лично посетите веб-сайт, прежде чем рекомендовать его для просмотра студентам. Хорошо также ставить закладки на веб-сайты до того, как приглашать студентов посетить тот или иной URL.



5. Выводы

Информационно-коммуникационные технологии или ИКТ, изменили современный стиль жизни. Они предоставляют нам возможность общения в реальном времени, безграничный и практически беспредельный доступ к информации и широкому спектру инновационных услуг.

В то же время они создают новые возможности для эксплуатации и оскорблений. Без соответствующих мер защиты дети, которые наиболее активно используют интернет, рискуют получить доступ к жестоким, сексуальным и другим вызывающим беспокойство изображениям.

Без соответствующего стремления к созданию безопасной киберсреды, мы сделаем ошибки в воспитании наших детей. Несмотря на то, что повсеместно растет осведомленность о рисках, связанных с небезопасным использованием ИКТ, все еще остается огромное поле деятельности.

Следовательно, очень важно, чтобы родители и учителя имели возможность принять решение о том, что приемлемо и безопасно для их ребенка, а также о том, как вести себя ответственно, используя ИКТ.

Работая вместе, родители, учителя и дети смогут воспользоваться преимуществами ИКТ, сведя к минимуму возможные опасности для детей.

Мы надеемся, что эти руководящие указания содержат ясную и исчерпывающую информация по защите ребенка в онлайновой среде, о рисках, которым могут подвергаться дети, и о том, что родители и учителя могут сделать для того, чтобы защитить и помочь своим детям понять, как воспользоваться массой преимуществ, которые предоставляют ИКТ, с минимум потенциальных опасностей.

Справочные документы и источники для дополнительного чтения

Children's Online Privacy Protection Act (COPPA) http://www.coppa.org/coppa.htm

Cyberpeace Initiative, доступен по адресу: http://www.smwipm.cyberpeaceinitiative.org

Cyril. A. Wantland, Subhas C. Gupta, Scott A. Klein, Safety considerations for current and future VR applications, доступен по адресу: http://www.webmed.com/i-med/mi/safety.html (последний раз посещался 4 сентября 2008 года).

'Are ads on children's social netwrking sites harmless child's play or virtual insanity?', The Independent, 2 июня 2008 г., доступен по адресу: http://www. independent.co.uk/news/media/areads- on-children-social-networkingsites- harmless-childs-play-or-virtualinsanity- 837993.html (последний раз посещался 11 июня 2008 года).

'Children's social-networking sites: set your little monsters loose online', Telegraph.co.uk, 17 ноября 2007 год, доступен по адресу: http://www.telegraph.co.uk/connected/main.jhtml?xml=/connected/2007/11/17/dlchildren17.xml (последний раз посещался 10 июня 2008 года).

CBC News, Cyber-bulliying, 2005, доступен по адресу: http://www.cbc.ca/ news/background/bulliying/cyber_ bulliying.html (последний раз посещался 4 сентября 2008 года).

Child Exploitation and Online Protection Centre (CEOP): Think You Know, доступен по адресу: http://www.thinkuknow.co.uk/parents/gaming/ bad.aspx (последний раз посещался 4 сентября 2008 года).

Children, Adolescents, and Television, American Academy of Pediatrics, Pediatrics, Vol. 107, No. 2, февраль 2001 г., доступен по адресу: http://aappolicy.aappublications.org/cgi/content/full/pediatrics;107/2/423 (последний раз посещался 10 сентября 2008 года).

Cyber-bulliying: Developing policy to direct responses that are equitable and effective in addressing this special form запугивания, Canadian Journal of Educational Administration and Policy, Issue n. 57, 18 декабря 2006 г., доступен по адресу: http://www.umanitoba.ca/publications/cjeap/articles/ brown_jackson_cassidy.html (последний раз посещался 2 сентября 2008 года).

eModeration, Virtual World and MMOG Moderation: Five techniques for creating safer environments for children, май 2008 г., доступен по адресу: http://www.emoderation.com/news/press-release-virtualworld- and-mmog-whitepaper (последний раз посещался 22 июля 2008 года).

Entertainment & Leisure Software Publishers Association (ELSPA), Unlimited learning – Computer and video games in the learning landscape, доступен по адресу: http://www.elspa.com/ assets/files/u/unlimitedlearningtheroleofcomputerandvideogamesint_ 344.pdf (последний раз посещался 26 августа 2008 года).

ENISA, Дети в виртуальных мирах – Что следует знать родителям, сентябрь 2008 г., доступен по адресу: http://www.enisa.europa.eu/doc/pdf/deliverables/ children_on_virtual_worlds..

Gauntlett, David and Lizzie Jackson, Virtual worlds – Users and producers, Case study: Adventure Rock, Communication and Media Research Institute (CAMRI), University of Westminster, UK, доступен по адресу: http://www.childreninvirtualworlds.org.uk/pdfs/Gauntlett_and_Jackson_May_2008.pdf

Home Office, Home office task force on child protection on internet – Good practice guidelines for the providers of social netwrking and other user interactive services 2008 г., доступен по адресу: http://police.homeoffice.gov.uk/publications/operational- policing/social-networkingguidance? view=Binary (последний раз посещался 16 июня 2008 года).

Home Office, Good practice guidance for the providers of social netwrking and other user interactive services 2008 г., доступен по адресу: http:// police.homeoffice.gov.uk/publications/ operational-policing/ socialnetworking- guidance (последний раз посещался 12 сентября 2008 года).

Home Office, Good Practice Guidance for the Moderation of Interactive Services for Children, доступен по адресу: http://police.homeoffice.gov.uk/ publications/ operational-policing/ moderation-document-final.pdf (последний раз посещался 12 сентября 2008 года).

http://disney.go.com/fairies/pixiehollow/ comingSoon.html (последний раз посещался 26 августа 2008 года).

http://www.redherring.com/Home/24182 (последний раз посещался 10 июля 2008 года).

Internet Watch Foundation: Protection Online http://www.iwf.org.uk/public/ page.36.htm

Keith, Stuart, 'SpongeBob is the real threat to our children online', The Guardian, 10 апреля, 2008 г., доступен по адресу: http://www.guardian.co.uk/technology/ 2008/apr/10/games.news (последний раз посещался 10 июля 2008 года).

Kirriemuir J., A Survey of the Use of Computer and Video Games in Classrooms, Nesta Futurelab Series, 2002, доступен по адресу: http://ccgi.goldingweb.plus.com/blog/wp-content/ Games_Review1.pdf (последний раз посещался 2 сентября 2008 года).

Kramer, Staci D., Disney Acquires Club Penguin; $350 Million Cash, Possible $350 Million Earnout, paidContent.org, 1 August 2007 год, доступен по адресу: http://www.paidcontent.org/entry/419-disney-acquiresclub- penguin-in-deal-values-at-700- million-to-be-brande/ (последний раз посещался 10 июля 2008 года).

Mediashift, Virtual Worlds for Children Entwined with Real World, доступен по адресу: http://www.pbs.org/mediashift/ 2007/06/your_take_roundupvirtual_ world.html (последний раз посещался 28 августа 2008 года).

Microsoft, How to help your children' use social netwrking Web sites more safely, 9 ноября 2006 г., доступен по адресу: http://www.microsoft.com/ protect/family/activities/social.mspx (последний раз посещался 11 июня 2008 года).

NSPCC: Children and Internet http://www.nspcc.org.uk/whatwedo/mediacentre/mediabriefings/ policy/children_and_the_internet_ media_briefing_wda49338.html

The Children's Charity: Net Smart Rules http://www.nch.org.uk/information/ index.php?i=135 Virtual Worlds Management, Disney.com Launches Games and Virtual Worlds Portal; Mobile Widgets, 14 August 2008 г., доступен по адресу: http://www.virtualworldsnews.com/2008/08/disneycom-launc.html (последний раз посещался 26 августа 2008 года).

Virtual Worlds Management, Virtual Worlds Managements Youth Worlds Analysis, 22 August 2008 г., доступен по адресу: http://www.virtualworldsmanagement.com/2008/youthworlds0808.html (последний раз посещался 25 августа 2008 года).

Virtual Worlds News, Virtual World 125,000 Children Fight Obesity in Whyville, доступен по адресу: http://www.virtualworldsnews.com/2007/06/ virtual_world_h.htm (последний раз посещался 4 сентября 2008 года).

Программы посла для обучения инструкторов – на различных узлах имеются хорошие примеры таких программ. http://www.thinkuknow.co.uk/ teachers/training.aspx http://www.saferinternet.at/tipps/ fuer-eltern/

Образовательные материалы. Существует множество отличных доступных ресурсов для доставки сообщения по электронной безопасности. Приведенные далее перечни не являются исчерпывающими, и дополнительные ресурсы можн найти по адресу: http://www.saferinternet.org/ ww/en/pub/insafe/resources.cfm.

http://www.digizen.org/cyberbulliying/ film.aspx – отличный ресурс, используемый несколькими сайтами для борьбы с запугиванием.

http://www.internetsanscrainte.fr/le-coin-des-juniors/dessin-animedumois Vinz et Lou – множество французских мультфильмов, направленных на повышение осведомленности в вопросах электронной безопасности.

http://www.cyberethics.info/cyethics2/page.php?pageID=25&mpath=/35 содержит широкий спектр советов для учителей.

http://www.easy4.it/content/category/ 13/59/104/ материалы с итальянского сайта, предназначенные для помощи учителям.

http://www.teachtoday.eu/en/Lesson-Plans.aspx. На этом сайте представлены планы уроков, разработанные для использования в школах. Сайт постоянно обновляется и вскоре будет доступно еще больше планов.

http://dechica.com игра для повышения осведомленности для маленьких детей, разработанная в Болгарии.

www.microsoft.com/cze/athome/bezpecnyinternet – флеш-версия развлекательной брошюры о том, как безопасно пользоваться интернетом, опубликованной компанией Microsoft. Распространялась во время Дня безопасного интернета 2009 года.

www.tietoturvakoulu.fi – Безопасное использование интернета и тест "Будь умным в Сети".

Видеозапись интервью с латвийскими известными людьми, которые выражают свое мнение и личный опыт в деле онлайнового запугивания. Язык(и): Больше интервью на латвийском: Video 2 (TV show star):

http://www.youtube.com/watch?v=QttMrRABnR0&feature=related - Video 3 (dancer):

http://www.youtube.com/watch?v=3cPRlhQDJAg&feature=related - Video 4 (rally driver):

http://www.youtube.com/watch?v=PodsmBjrE6Y&feature=related - Video 5 (politician): http://www.youtube.com/watch?v=4_xrUvDQaIY&feature=related - Video 6 (singer):

http://www.youtube.com/watch?v=usqpmAHjHQ4 www.tietoturvakoulu.fi. Используя этот онлайновый тест, родители могут проверить свои знания в сфере информационного образования. Языки: финский и шведский.

http://www.medieradet.se/Bestall--Ladda-ner/filmrummet – часть веб-сайта ШВедского совета по средствам информации, содержащий видеоизображения. Язык(и): шведский, и некоторые части на английской.

http://www.lse.ac.uk/collections/EUKidsOnline/ Европейское исследование проблем культуры, контекста и рисков в сфере безопасного использования детьми интернета и новых средств информации.

http://www.nortononlineliving.com/ содержит обзор тенденций в различных странах.

http://www.pewinternet.org/Pew. Содержит множество отчетов об использовании интернета и связанных с ним технологий. Несмотря на то, что сайт находится в США, на нем приводятся тенденции, которые берут свое начало в США и со временем приходят в Европу.

http://www.unh.edu/ccrc/ исследование Дэвида Финкельора о тенденциях арестов интернет-хищников, в котором предполагается, что не существует реальных доказательств, подтверждающих высказывания о том, что интернет создает больше интернет-хищников.

http://www.webwise.ie/article.aspx?id=10611 исследование, выполненной ирландским сайтом.

http://www.childnet-int.org/youngpeople/

www.kidsmart.org.uk

www.chatdanger.com

Приложение 1

Встроенная защита

Все компьютеры – и PC и Mac – имеют встроенные во все новые операционные системы возможности родительского контроля, включая системы Windows Vista и Leopard. Если вы собираетесь обновить свою операционную систему, то такое переключение может помочь вам сэкономить на покупке дополнительных программ контроля.

Для использования программ контроля на своем компьютере, сначала создайте персональный аккаунт пользователя для каждого из своих детей. Сверьтесь с руководством использования компьютера, если вы не знаете, как это делается.

Для пользователей компьютеров Mac: затем в меню Apple выбираете "System Preferences" и кликаете на надпись "Accounts". Для аккаунта каждого из своих детей кликните по ссылке "Parental Controls" и вы получите список категорий – Mail, Safari и т. д., которые вы можете ограничить или контролировать.

Если у вас стоит система Leopard, то, кроме прочего, вы можете записывать обмен мгновенными сообщениями и указывать, с кем ваш ребенок может общаться по электронной почте или через iChat. Вы также можете ограничить время работы компьютера. Например, можете установить автоматическое выключение компьютера в 8 часов вечера.

Для пользователей Windows: программы родительского контроля доступны через панель управления. Ищите "Аккаунты пользователя" и "Семейную панель управления безопасности". Используя Windows Vista, вы получаете выбор ограничений для работы в интернете и также возможность получать отчеты об использовании компьютера вашим ребенком. Вы можете указать определенные часы суток как не рабочие, а также блокировать видеоигры и другие программы.

Неважно, какую систему вы используете, большинство браузеров (Safari, Firefox, и т. д.) поддерживают автоматический журнал, который показывает, какие сайты посещались. Сверьтесь с руководством пользователя, чтобы узнать, как проверить журнал, если вы это знаете не очень хорошо. Удостоверьтесь, что вы проверяете все браузеры на вашем компьютере, если их несколько. И знайте, дети могут узнать, как удалить журнал, чтобы скрыть свои следы, поэтому задавайте вопросы, если увидите, что журнал удален кем-то помимо вас.

Нужда помощь? И у Apple (Mac), и у Microsoft (Windows) имеются онлайновые справочники и подробные информационные страницы на их сайтах – просто наберите в Google "родительский контроль" и "Apple" или "Microsoft", чтобы их найти.

Помните, что любая защита, которую вы обеспечиваете своим детям, конечно, будет неполной. Необходимо как можно больше общаться с детьми, говорить с ними о проблемах защиты ребенка в онлайновой среде.

Приложение 2

Декодированный язык мгновенных сообщений

Сокращения и кодовые слова ускоряют обмен мгновенными и текстовыми сообщениями, но они также маскируют то, что говорят люди! Соберитесь! Вот некоторые общеупотребительные выражения:

ADIH: Another day in hell – Еще один день в аду

A/S/L: Age, sex, location – Возраст, пол, место

BTDT: Been there done that – Был там, сделал это

CULTR: See you later – Пока

GTFO: Get the f-ck out (expression of surprise) – Выражает удивление

H8: Hate – Ненависть

ILY or 143 or <3: I love you – Я тебя люблю

JK or J/K: Just kidding – Просто шучу

KWIM: Know what I mean? – Понимаешь, что я имею в виду?

LLS: Laughing like sh-t – Хохочу до упаду

LMIRL: Let's meet in real life – Давай встретимся в реальном мире

LYLAS (B): Love you like a sister (brother) – Люблю как сестру (брата)

NIFOC: Naked in front of computer – Голый перед компьютером

PAW or PIR or P911: Parents are watching or Parent in room (drop the subject) – Родители смотрят или Родители в комнате (оставим эту тему)

POS: Parent over shoulder (может означать также "piece of sh-t,") – Родители смотрят (иди выражение обиды)

Pr0n: Intentional misspelling of "porn" – Международная орфографическая ошибка в слове "порно"

STFU: Shut the f-ck up – Выражение удивления

TMI: Too much information – Слишком много информации

TTFN: Ta ta, for now (goodbye) – Пока

WTF: What the f-ck? – Что случилось?

Международный союз электросвязи
Place des Nations
CH-1211 Geneva 20
Switzerland
www.itu.int/cop

Отпечатано в Швейцарии
Женева, 2011 г.

При поддержке:

CHIS

ins@fe

CYBER Peace Initiative

enisa European Network and Information Security Agency