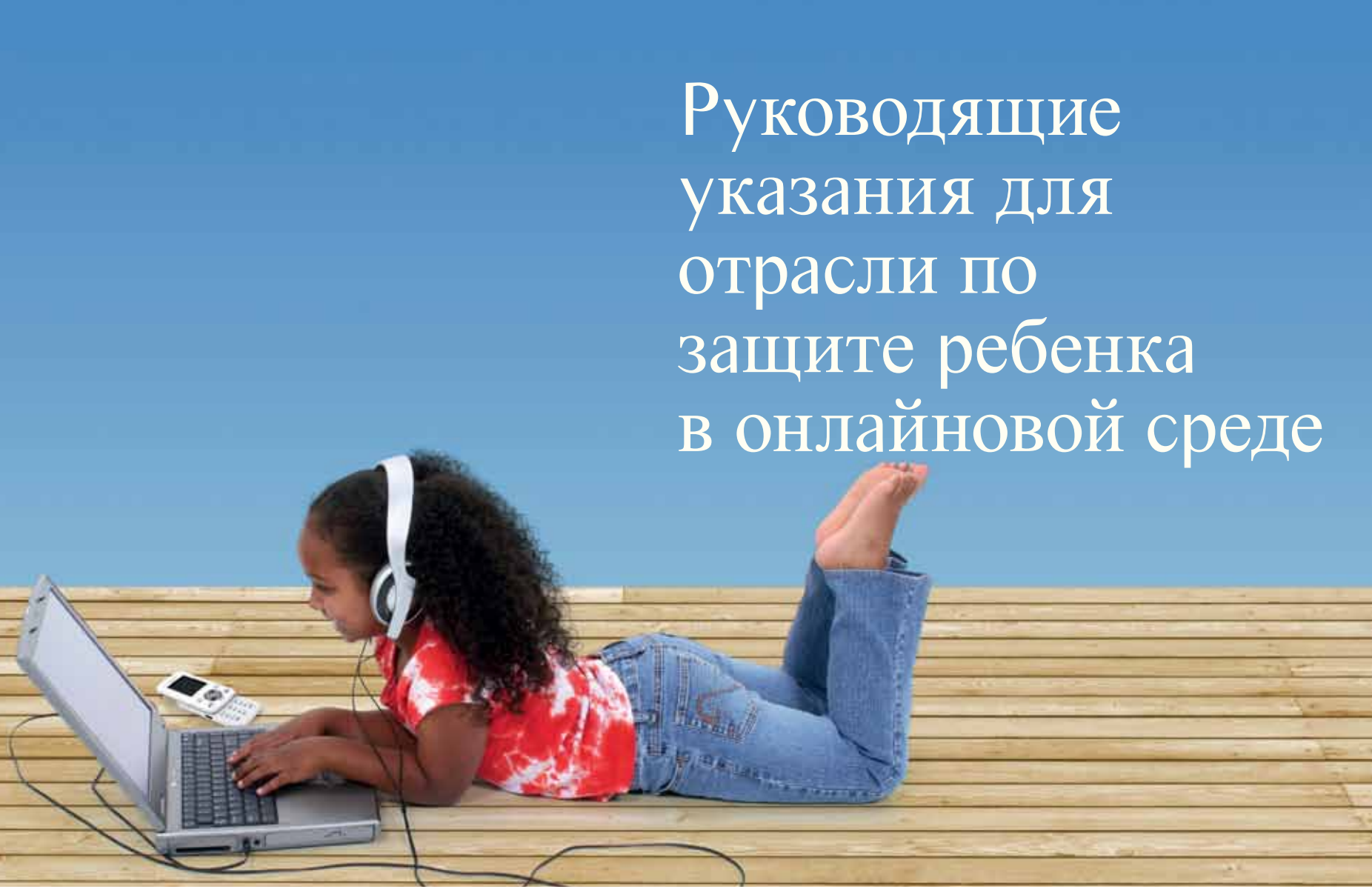
Руководящие указания для отрасли по защите ребенка в онлайновой среде



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 самоотверженность. МСЭ благодарит всех следующих авторов, потративших свое драгоценное время и знания (перечислены в алфавитном порядке):

- Кристина Буети (Cristina Bueti) – МСЭ
- Джонн Карр (John Carr) – Детская благотворительная коалиция за безопасность интернета
- Наташа Джексон (Natasha Jackson) и Дженни Джонс – Ассоциация GSM (GSMA)
- Нериша Кайе (Nerisha Kajee) и Роб Вортвик (Rob Warthwick) – Vodafone
- Жиакомо Маззоне (Giacomo Mazzone) – EBU на основании документов, предоставленных Марком Готчильдом (Marc Goodchild) и Джклиан Солее (Julian Coles) – оба из BBC
- Майкл Моран (Michael Moran) – Интерпол
- Брайан Маньо Лонгве (Brian Munyao Longwe) – AfrISPA
- Лоренцо Пупилло (Lorenzo Pupillo) и Рокко Маммолити (Rocco Mammoliti) – Telecom Italia

Авторы хотели бы поблагодарить Кристин Квинь (Kristin Kvigne) из Интерпола за подробный разбор и комментарии.

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

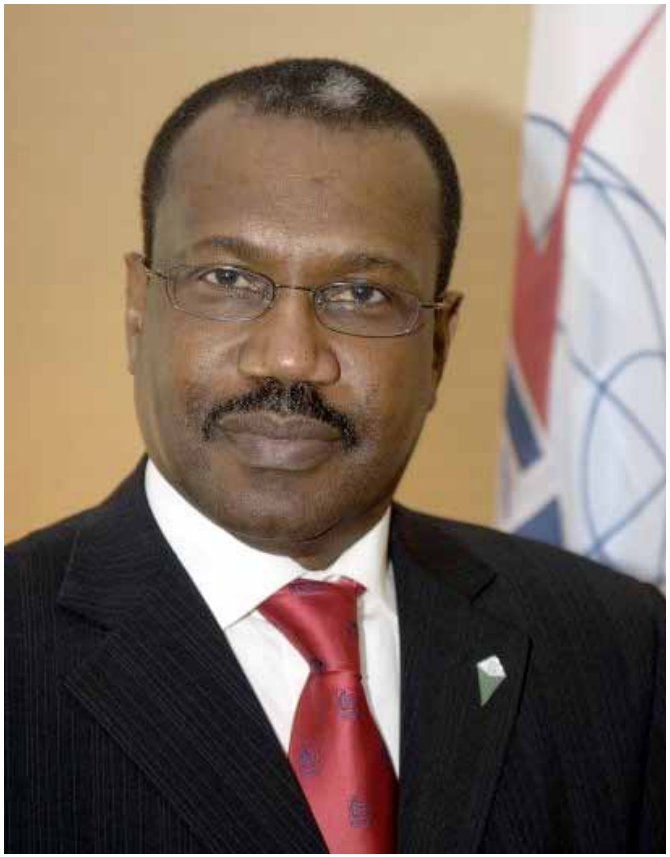
Дополнительная информация по этому проекту Руководящих указаний размещена по адресу http://www.itu.int/cop/ и будет регулярно обновляться.

Если у вас есть какие-либо замечания, или вы хотели бы предоставить дополнительную информацию, пожалуйста, свяжитесь по адресу: cop@itu.int.

Содержание


“Защита детей в онлайновой среде является глобальной задачей, поэтому 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.

Участники сектора: радиовещательные организации, поставщики услуг интернета (ISP) или операторы подвижной связи – 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)

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 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.

Краткое содержание

Настоящие Руководящие указания были подготовлены в рамках инициативы Защиты детей в онлайновой среде (COP)[1] с целью создания основы для безопасного и надежного кибермира не только для детей, живущих сегодня, но и для будущих поколений.

Представленная в этих Руководящих указаниях информация была создана МСЭ и командой авторов из лидирующих организаций, действующих в секторе ИКТ, например, GSMA, Интерпол, Afrispa, EBU, Telecom Italia, Детская благотворительная коалиция за безопасность интернета и Vodafone.

Множество партнеров, которые собрались вместе для совместной деятельности по созданию этого документа, сами по себе являются свидетельством быстрых изменений, которые произошли в интернете, в то время как цифровая революция продолжает набирать обороты.

Сегодня во многих странах наблюдается конвергенция, и нет никаких сомнений, что она несет с собой множество новых проблем. Сотрудничество и партнерство важны для прогресса. Ни один сектор отрасли не имеет монополии на знание или мудрость. Все мы учимся друг у друга.

МСЭ вместе с другими авторами отчета призывает все заинтересованные стороны поощрять принятие правил и стандартов, которые защитят детей в киберпространстве и поощрять их безопасный доступ к онлайновым ресурсам.

Мы надеемся, что это приведет не только к созданию более охватывающего информационного общества, но также даст возможность Государствам – Членам МСЭ выполнять свои обязательства по отношению к защите и реализации прав детей, в соответствии с Конвенцией Организации Объединенных Наций о правах ребенка, принятой в соответствии с Резолюцией 44/25 Генеральной Ассамблеи ООН от 20 ноября 1989 года и Итогового Документа ВВУИО.

[1] www.itu.int/cop

Руководящие указания для отрасли

В этом разделе приведены Руководящие указания для отрасли по защите детей в онлайновой среде. Для того чтобы сформулировать национальную стратегию, направленную на защиту детей в онлайновой среде, главы отрасли должны принимать во внимание следующие стратегии в упомянутых ниже областях:

		Ключевые области, требующие рассмотрения
Отрасль ИКТ в целом		Существует острая необходимость в общих действиях, которые выходят за рамки отдельных организаций ИКТ. Они включают в себя:
	1	Разработку взаимодействующих стандартов и соответствующих рекомендаций для защиты детей в онлайновой среде. Целью является создание подхода с широкими возможностями совместного использования, который будет поддерживаться всей отраслью.
	2	Оценку того, какие существуют возможности и варианты для всемирных скоординированных и согласованных действий для защиты детей в онлайновой среде. Следует уделить внимание созданию таких возможностей, например, мониторинг, предупреждение и управление происшествиями, которые облегчат сбор информации об угрозах и обмен ею между различными участниками.
	3	Определение общих сторон для различных секторов (радиовещательные организации, интернет, подвижную связь) с целью создания Кодексов поведения, или правил действий для помощи Государствам – Членам МСЭ в организации более эффективного сотрудничества с частным сектором/отраслью.
	4	Создание правительствами и частным сектором/отраслью совместных организаций для обмена информацией и разработка конкретных возможностей, направленных на снижение рисков и расширение потенциала использования ИКТ детьми.

		Ключевые области, требующие рассмотрения
Радиовещательные организации	5	Разработка общих правил, относящихся к системам жалоб. Цель состоит в том, чтобы избежать ситуации, когда к собственным внутренним системам радиовещательной организации добавляются внешние функции по работе с жалобами, которые, по всей вероятности, создают больше беспорядка с пользователями или риск перегрузить полицию и другие службы большим количеством запросов, с которыми их службы не должны или не имеют возможности справляться.
	6	Разработка общих стандартов и рекомендаций. Цель состоит в том, чтобы создать подход к защите детей в онлайновой среде с широкими возможностями совместного использования. Он будет использоваться в рамках всей отрасли.
	7	Создание общеотраслевого проекта по разработке более надежных процедур по получению родительского согласия на доступ их детей к зависящему от возраста содержанию, чувствительное к возрасту как минимум на региональной основе.
		Ключевые области, требующие рассмотрения
Поставщики услуг интернета (ISP)		В следующих рекомендациях представлены руководящие указания для отрасли интернета и поставщиков услуг интернета (ISP), позволяющие поддерживать более безопасные условия для юных пользователей. Каждая указанная ниже область, требующая рассмотрения, должна стать частью более подробного руководства по защите пользователя ответственных поставщиков онлайновых услуг.
	8	Стратегические задачи отрасли интернета по защите детей в онлайновой среде должны заключаться в снижении доступности и запрете доступа к сайтам с опасным или незаконным содержанием и поведением. ISP также должны предоставлять детям и их родителям информацию и простые в использовании инструменты, позволяющие управлять их действиями в интернете таким образом, чтобы снизить потенциальную опасность.
	9	Языки и терминология интернет-сайтов и служб Web 2.0 должны быть доступны, понятны и значимы для всех пользователей, включая детей, молодых людей, родителей и опекунов, особенно в том, что касается Условий использования сайта, политики конфиденциальности и механизмов отчетности.
	10	Отчеты о проблемах, злоупотреблении или незаконном поведении: для поставщиков услуг очень важно создать надежные процедуры по работе с жалобами. В частности, жалобы на сайты, содержащие агрессивный или недопустимый контент, должны быстро рассматриваться, и по возможности проблемный контент должен сразу же удаляться. По возможности поставщики услуг должны рассмотреть возможность создания механизмов, например, ссылки на отчет о злоупотреблении или маркировки профилей, которые могут быть недопустимы или подвергают детей или подростков риску, и должны иметь возможность при необходимости передать любой отчет органам охраны правопорядка.

		Ключевые области, требующие рассмотрения
	11	Поставщики услуг должны рассмотреть возможность создания по умолчанию возможности отчета на всех веб-страницах и для всех веб-услуг, предлагаемых ISP, при помощи кнопки "отчет о злоупотреблении", если это возможно. Может быть создана общая, узнаваемая кнопка, которая всегда находится одном и том же месте экрана. Механизм отчета может быть расширен при помощи предложения технических решений пользователю, отправляющему отчет, например, возможности добавления скриншота, статистических данных о соединении, список запущенных процессов и пр., и информации для пользователя о том, какая информация ему будет нужна для включения в отчет, чтобы сделать его эффективным.
	12	Поставщики услуг должны рассмотреть возможность того, как доступным и легко понятным языком указать "какое поведение является и не является допустимым в услуге", особенно для юных пользователей, их родителей и опекунов. Предполагается, что эта информация должна предоставляться дополнительно, а также быть включена в Условия использования.
	13	Поставщики услуг должны продолжить повышать эффективность технологий, которые определяют и подтверждают возраст пользователей. Целью должна быть реализация соответствующего решения, пригодного для их конкретной услуги (это будет особенно важно, когда рассматриваемая услуга является предметом правовых запретов для определенного возраста), с тем чтобы это решение было гибким в правовом и техническом отношении и, что более важно, создавало более безопасные и надежные услуги интернета. Такие решения могут применяться по-разному для предотвращения доступа лицами, не достигшими определенного возраста, и предоставления контента или услуг, недопустимых по возрасту, или действий для предоставления услуг, предназначенных только для детей без родителей.
	14	Поставщики услуг должны продолжить повышать эффективность технологий, которые определяют и подтверждают возраст пользователей. Целью должна быть реализация соответствующего решения, пригодного для их конкретной услуги (это будет особенно важно, когда рассматриваемая услуга является предметом правовых запретов для определенного возраста), с тем чтобы это решение было гибким в правовом и техническом отношении и, что более важно, создавало более безопасные и на дежные услуги интернета. Такие решения могут применяться по-разному для предотвращения доступа лицами, не достигшими определенного возраста, и предоставления контента или услуг, недопустимых по возрасту, или действий для предоставления услуг, предназначенных только для детей без родителей. Далее приведен "контрольный список" предложенных областей, требующих рассмотрения операторами подвижной связи при пересмотре их подхода к защите детей, как в том, что касается создания безопасных и подходящих условий подвижной связи для маленьких пользователей, так и в том, что касается противодействия возможности злонамеренного использования их услуг с целью размещения или распространения незаконного контента, связанного с сексуальным насилием над детьми.

		Ключевые области, требующие рассмотрения
	15	При предложении контента и услуг, которые подходят по возрасту не для всех пользователей, обеспечьте такое положение дел, при котором содержание классифицируется в соответствии с национальными ожиданиями, отвечает существующим стандартам в аналогичных средствах информации и предлагается вместе с подтверждением возраста, когда это возможно.
	16	Если возможно, работайте вместе с другими операторами, представленными на местном рынке с целью согласования и продвижения набора отраслевых обязательств относительно того, какой контент для какого возраста является уместным.
	17	Предоставляйте инструменты, которые дают пользователю или родителю/воспитателю возможность управления доступом к контенту. Опять же, это должно отвечать национальным ожиданиям и стандартам в аналогичных средствах информации.
	18	Четко определяйте характер предлагаемого контента и услуг, чтобы пользователи могли принимать обоснованное решение об использовании ими контента, и о любых принимаемых ими обязательствах, например, о минимальном периоде подписки.
	19	Поддерживайте родителей в представлении о полном спектре контента услуг подвижной связи, которыми могут пользоваться их дети, чтобы они могли дать своим детям рекомендации по правильному использованию приложений подвижной связи.
	20	Обучайте пользователей тому, как обращаться с вопросами, касающимися использования подвижной связи в целом – включая такие области, как спам, воровство и неподходящие контакты, например запугивание – и уверьте их в том, что вы предлагаете пользователям способы, помогающие справиться с любой проблемой.
	21	Используйте ваши Условия использования, для того чтобы однозначно определить позицию вашей компании в отношении злонамеренного использования ее услуг для хранения или передачи контента с сексуальным насилием над детьми и обязательства компании в содействии расследований любых злоупотреблений, провидимых органами охраны правопорядка, в соответствии с национальным законодательством; сформируйте процедуры Уведомления и Удаления (NTD), или эквивалентные им; поддерживайте национальные горячие линии или их эквивалент, где они существуют.

1. Исходные данные

Современный цифровой мир изменил индивидуальный уклад жизни по всему миру. Компьютерная отрасль давно была полностью цифровой, отрасль электросвязи уже практически полностью стала цифровой, и сектор широкополосной связи далеко продвинулся в сторону цифровизации. Постоянный доступ в интернет стал нормой, люди тратят в цифровых средствах информации все больше времени, используя их чаще любых других средств информации.

Каждый день от Китая до Италии жизнь наполнена СМС, электронной почтой, чатами, онлайновыми знакомствами, многопользовательскими играми, виртуальными мирами и цифровыми мультимедийными продуктами.

Хотя эти технологии для многих означают больше комфорта и развлечений, регуляторные органы и пользователи часто на шаг отстают от быстро появляющихся инноваций в этой области.

Более того, поскольку многие каналы для доставки услуг диверсифицируются, бизнес этого сектора как традиционный, так и новый, сталкивается с множеством новых дилемм.

Совместная деятельность отрасли

В современном конвергирующем информационном мире традиционные различия между различными частями отраслей электросвязи и мобильной телефонии, между интернет-компаниями и радиовещательными организациями быстро исчезают или становятся незначительными. Конвергенция сводит эти до сих пор раздельные цифровые потоки в одно русло, которое достигает миллиардов людей во всех частях света. Учитывая такую ситуацию, МСЭ в сотрудничестве с GSMA, Telecom Italia, Европейским радиовещательным союзом, Интерполом, Детской бла-

готворительной коалицией по интернет-безопасности, Vodafone и Afrispa подготовил эти Руководящие указания для отрасли по защите детей в онлайновой среде. Их целью является предоставление всем сегментом отрасли общей основы для работы над общей задачей, заключающейся в том, чтобы сделать интернет максимально безопасным для детей и молодых людей, например, путем создания кодексов поведения или авторитетных источников советов и указаний.

Поставщики услуг интернета, в частности, давно решили, что они несут особую ответственность за защиту детей в онлайновой среде. Это в основном происходит из-за того, что ISP действуют и как линия связи, предоставляя доступ в интернет, и как хранилище, так как они предоставляют услуги хостинга, кэширования и хранения. То же самое касается сетей мобильной телефонии, многие из которых расширяют свои функциональные возможности далеко за пределы традиционных услуг голосовой связи и передачи данных. Радиовещательные организации также стали крупными участниками рынка интернета, предоставляя многие онлайновые услуги, которые в прошлом были связаны только с ISP или компаниями, предоставляющими онлайновый хостинг.

Однако из-за большого числа представленных на рынке торговых марок, обычно созданных за много лет до появления интернета как массового пользовательского продукта, сайты радиовещательных организаций обычно привлекают большое количество последователей.

Каждый сектор, работающий вместе в этом совместном проекте, вносит свой опыт и свои собственные особые области знаний. Работая вместе, таким образом, объединяя знания и опыт, отрасль в целом получает возможность предоставления более безопасных услуг интернета для всех, но больше всего, для детей и подростков.

2. Классификация содержания и услуг

Мнение о том, что не весь контент и не все услуги подходят для всей аудитории, очень хорошо понимается в "оффлайновом"мире: например, фильмы и игры имеют возрастные ограничения, а время трансляции телепрограмм, содержащих сцены насилия или сексуальные сцены, ограничивается.

Когда содержание онлайновой версии практически совпадает с "оффлайновой", например, игра или фильм, которые отличаются только параметрами канала доступа, то можно использовать существующие ограничения и классификации. Однако когда содержание новое или измененное, поставщики онлайнового контента и услуг должны найти способы оповестить своих пользователей о природе этого контента и возрастных ограничениях целевой аудитории.

В случаях с более традиционны контентом, например, видеоклипами, часто можно применить возрастные ограничения, определенные посредством сравнительного анализа стандартов с существующими национальными или, возможно, региональными рамками в зависимости от уровня совместно используемой социальной чувствительности, например, игр или фильмов. Однако постоянно растущее число интерактивных услуг, таких как форумы, чаты, социальные сети и сервисы, допускающие создание контента пользователем, также могут создавать для юных пользователей риски, связанные не только с неподходящим по возрасту содержанием, но и неподобающим поведением, например, запугиванием, и контактами, например, соблазнением.

Все эти вопросы рассматриваются в подразделах ниже. В подразделе, посвященном радиовещательным организациям, рассматривается вопрос создания традиционного контента, доступного в новой

среде передачи, в подразделе, посвященном поставщикам интернета, рассматриваются вопросы контента, контактов и поведения, связанные с управлением нетрадиционными онлайновыми услугами, а в подразделе, посвященном операторам подвижной связи, представлен обзор того, какой подход к вопросу классификации и управления контентом и услугами подвижной связи применяют операторы по всему миру.

Радиовещательные организации

Телевизионные радиовещательные организации традиционно используют линейный "радиовещательный"характер просмотра телепрограмм, решая проблемы возрастных ограничений для контента посредством расписания с контролем времени: например, передавая контент, который подходит только для старших подростков или взрослых, поздно вечером или ночью (после "водораздела"(время после 21.00)), когда маленькие дети спят.

Однако так как радиовещательные организации все чаще делают содержание своих программ доступным в онлайновом режиме на нелинейной основе "по запросу", когда нельзя надеяться на прямой родительский контроль и расписание с контролем времени более не применимо, радиовещательные организации исследуют способы организации доступа к своим программам на основе возраста.

Исследования показали, что в целом родители хотят знать о видах контента, которые могут вызвать тревогу, например, нецензурные выражения или насилие, а не просто получить возрастные ограничения.

Поэтому некоторые радиовещательные организации разработали систему обозначений, например, BBC разработала систему обозначений "G" (от Guidance – указание), где символ "G" появляется на экране в те моменты, когда часть содержания содержит неоднозначный материал, а сущность содержания отражается в текстовом виде в кратком обзоре программы. Наличие символа "G"используется для запуска системы родительского контроля с PIN-кодом, если она активирована.

Примечание. – Если не сказано обратного, термин "радиовещательные организации"в данном документе конкретно относится к поставщикам традиционного содержания радиовещательного типа, в том смысле, что "радиовещательная организация"имеет творческий и редакторский контроль над доступным содержанием, вне зависимости от того, является ли оно "эфирным"или, как рассматривается в данном документе, онлайновым. Этот термин не должен включать поставщиков услуг, которые позволяют публиковать содержание, созданное другими, такие организации подпадают в категорию поставщиков услуг интернета.

Ситуационное исследование: Британская радиовещательная компания (BBC) – Соединенное Королевство

Используя свое предложение услуги iPlayer, которая предоставляет онлайновый доступ к программам BBC на нелинейной (или "по запросу") основе, а также в настоящее время составляет 9% всего трафика интернета в Соединенном Королевстве, BBC создала важный пример управления ответственной доставкой контента, чувствительного к возрасту.

В настоящее время установка BBC iPlayer запрещена лицам моложе 16 лет. Кроме того, в момент регистрации пользователи информируются о защите PIN-кодом и должны принять решение о том, должен ли он ее активировать и в каких случаях. Если они отказываются от защиты PIN-кодом, им сообщают о том, как они могут активировать ее позже. Если программа не подходит для общего просмотра, т. е. не предназначена для всех возрастов, она включает в себя предупреждение – в данном случае, в тот момент когда пользователь решает загрузить ее, появляется знак "G"и текстовое сообщение, объясняющее характер содержания. Во время просмотра также демонстрируется текстовое сообщение и, прежде чем пользователь сможет просмотреть содержание, он должен ввести PIN-код, если он активирован. Любой, кто использует iPlayer без правильного PIN-кода, получает пояснительное сообщение о том, что ему не разрешен доступ к содержанию, отнесенному к категории "G".

В скором времени BBC представит потоковый контент для услуги iPlayer, и, где это допустимо, программы также будут содержать метку "G", и, прежде чем содержание можно будет просмотреть, будет показано текстовое сообщение. Система защиты PIN-кодом будет доступна с самого начала, и в настоящее время BBC ищет способы ее еще больше усилить, так как потоковое содержание и загрузка соединены в одну систему.

Система "G"(от Guidance – указание) BBC также была принята другими наземными радиовещательной организациями в Соединенном Королевстве, включая ITV, Channel Four и FIVE, для их онлайновых предложений "по запросу". BBC имеет очень четкую стратегию относительно поддержки детей с самого рождения до совершеннолетия при помощи трех сайтов, которые отражают разные уровни защиты, в зависимости от возраста, компьютерной грамотности, независимости и зрелости по мере их взросления, как и особые образовательные услуги, предлагаемые программой BBC Learning.

1 Веб-сайты CBeebies (www.bbc.co.uk/cbeebies) и CBBC (www.bbc.co.uk/cbbc) позволяют детям и их родителям или опекунам взаимодействовать с нами и друг с другом в безопасных, надежных и доступных условиях. Эти сайты предлагают высокое качество, привлекательное и соответствующее интерактивное содержание и примеры для детей и выступают в качестве трамплина к более подходящим внешним веб-сайтам для детей младше 12 лет.

2 Основное внимание направлено на помощь детям и предоставление им возможности создать более тесные взаимоотношения с BBC, брендами и персонажами, повысить полезность получаемых ими сведений, сопричастность, которую они ощущают, и влия-

ние, которое они имеют на CBeebies и CBBC. Чтобы достичь этого, сайты предлагают целый спектр новейших интерактивных инструментов и творческих возможностей для всех британских детей, с любыми способностями и образованием, предоставляя им пространство для размещения своих творений, мыслей и мнений. Кроме того, как часть программы Newsround, мы предлагаем специальную новостную онлайновую службу для детей, которая работает в режиме 24/7, и при помощи отделения PressPack мы активно привлекаем детей к обсуждению проблемных вопросов, которые их касаются.

3 Канал BBC Switch предоставляет онлайновое пространство для всех подростков, его содержание направлено на привлечение молодых людей, обращая внимание на их интересы и стимулируя их взаимодействие. На сайте размещены вспомогательные телевизионные и радиопрограммы и отдельное содержание. (www.bbc.co.uk/switch)

4 Канал BBC Learning предоставляет продукты, предназначенные для детей школьного возраста и охватывающие широкий спектр предметов и навыков. Указанные ниже продукты относятся к учебному плану или особым навыкам.

Bitesize – служба проверки и повторения всех главных предметов для детей в возрасте от 5 до 16 лет (www.bbc.co.uk/schools/ks3bitesize).

Blast – развитие творческих способностей подростков, в настоящее время направленный на творческие виды искусства, включая партнерство с молодежными художественными организациями (www.bbc.co.uk/blast).

Некоторые службы предназначены для использования в классе, другие все чаще напрямую используются учащимися дома или в школе без необходимости участия учителя.

BBC тесно сотрудничает с Ofcom (регуляторным органом Соединенного Королевства в области средств массовой информации и электросвязи) и многими радиовещательными организациями и поставщиками платформ для продвижения примеров передового опыта по присвоению обозначений; BBC также была активным участником Группы информационного контента (BSG). BBC также является ассоциированным членом Ассоциации предоставления услуг телевидения по запросу (ATVOD), саморегулируемого органа для услуг, предоставляемых по запросу.


Social
Networking

Поставщики услуг интернета

Как правило, контент интернета и услуги Web 2.0 – термины, относящиеся к растущему использованию интернета людьми с целью создания и распространения своего собственного контента, как в аудио-визуальной, так и в текстовой форме. Отдельные примеры служб Web 2.0 включают в себя:

- **Сайты с содержанием, созданным пользователем**, например, Википедия, блоги и сайты для размещения изображений, которые созданы специально, для того чтобы пользователи загружали, обменивались или просматривали их содержание.
- **Сайты общения в социальных сетях**, где пользователи имеют свои личные "профили", содержащие, например, информацию об их месте жительства, интересах и предпочтениях, например, в музыке, фильмах или книгах, или фотографии и видеоматериалы, музыкальные записи и ссылки на профили друзей. Также они могут иметь возможности для чата, обмена файлами, ведения блогов и дискуссионных групп.
- **Онлайновые сообщества и социальные миры**, где участники выбирают, настраивают или создают персонажей, которые называются "аватарами". Эти аватары могут строить дома, обставлять их мебелью, взаимодействовать с другими аватарами и даже обмениваться виртуальными деньгами, приобретая и продавая предметы в многопользовательском мире.
- **Онлайновые игры**, где игроки играют с другими, часто в сложных и обширных "игровых мирах", и где они могут взаимодействовать и общаться друг с другом в процессе игры.

Зачастую эти категории накладываются друг на друга, и сайты этих сетей все чаще рассматриваются как часть молодежной культуры, как об этом говорится в подробном и независимом обзоре Соединенного Королевства, рассматривающем угрозы для детей, связанные с интернетом и видеоиграми.

Полезно различать возможные риски, связанные с "контентом", "контактом" и "поведением", согласно структуре, предложенной проектом EU Kids Online[2]. Благодаря Web 2.0 и существенному увеличению интерактивности, теперь можно организовать общение по схеме один-с-одним, один-с-многими и многие-со-многими.

Это очевидно вызывает озабоченность по поводу нежелательных контактов и, в некоторых случаях, незаконного поведения. Проводить различия между контактом и поведением полезно для понимания отличий, сходства и возможных мер противодействия. Главное отличие проявляется в том, что "контакт" относится к ситуации, когда ребенок является получателем информации/сообщения ("жертвой"); а "поведение" относится к ситуации, когда ребенок является зачинщиком неподобающего поведения ("преследователем")[3]. Другие авторы добавили еще две категории, которые стоит иметь в виду: "торговля", которая относится к возможности того, что дети и молодые люди эксплуатируются нечистоплотными компаниями, которые пользуются неопытностью молодых людей, или это относится к проблемам, например, фишинга, когда

[2] www.eukidsonline.net/

Примечание. – В разделах, посвященных поставщикам услуг интернета, обсуждаются подходы, доступные для отрасли интернета в целом. Она включает в себя поставщиков услуг интернета и поставщиков электронных услуг/поставщиков содержания и услуг – все вместе они в этом документе называются поставщиками услуг интернета (ISP). По существу следует заметить, что не все рекомендации применимы ко всем ISP.

[3] Безопасность детей в цифровом мире: отчет исследования Byron Review (http://www.dcsf.gov.uk/byronreview/).

опять же молодые люди могут быть более уязвимы; наконец, могут возникнуть проблемы "зависимости", которые касаются способов, с применением которых некоторые дети и молодые люди могут быть одержимо увлечены технологией так, что это создает препятствия или преграду для их нормального развития отношений с другими людьми или участия в здоровой физической деятельности.

С точки зрения отрасли интернета, существует три стратегические задачи по обеспечению безопасности детей в интернете, которые требуют, чтобы отрасль и родители/опекуны несли коллективную ответственность за усиление безопасности детей в онлайновой среде:

- **Снижение уровня доступности**: снижает доступность опасного и неподходящего содержания, контактов и поведения (отрасль);
- **Ограничение доступа**: дает детям и их родителям эффективные инструменты управления неподходящим контентом (отрасль и семья);
- **Усиление устойчивости**: повышает устойчивость детей к материалам, которые они могут увидеть; дает детям возможность справиться с воздействием опасного и неподходящего содержания и контактов и дает родителям возможность помочь своим детям справиться с этими вещами, а родителям возможность эффективно действовать в ситуациях, когда их дети ведут себя опасно и неподобающим образом (родители).

Важным следствием природы интернета является то, что не существует одного определенного пункта, в котором может применяться содержательный контроль, в отличие от радиовещательной среды, где содержательный контроль осуществляет канал. Существует содержательный контроль, например, модерация сайтов с создаваемым пользователями контентом, но он распылен по "цепочке создания ценности интернета". Эта цепочка создания ценности состоит из создателя контента, агрегатора контента, поставщиков услуг интернета (ISP) и веб-хостинга, поставщиков услуг поставщиков услуг поиска, справочников и веб-услуг, абонентского устройства и т. д.

В каждом звене цепочки создания ценности имеется множество технических инструментов, которые могут помочь родителям управлять доступом их детей в интернет, например, ПО родительского контроля, безопасный поиск и подтверждение возраста на веб-сайтах.

Роль, которую играет отрасль интернета, работающая вместе с семьями, показана в следующем примере:

1 Веб-сайты с созданным пользователями контентом убирают опасные и неподходящие материалы, загруженные на их сайты.

2 Дети и родители сообщают владельцам веб-сайтов о найденных ими опасных и недопустимых материалах.

3 ISP блокируют доступ к незаконным материалам, например, изображениям насилия над детьми.

4 Родители устанавливают программное обеспечение для фильтрации опасного и недопустимого содержания.

5 Веб-сайты предоставляют ясные и хорошо видимые рекомендации о том, как остаться в безопасности.

6 Родители беседуют с детьми, а дети со своими друзьями и родственниками об электронной безопасности.

Снижение уровня доступности:

Задача снижения уровня доступности опасного и недопустимого контента, контактов и поведения может быть выполнена при помощи поставщиков услуг, предпринимающих следующие действия:

- Применяют эффективный **процесс модерации** контента, созданного пользователем, например, сервис MySpace после загрузки каждого изображения или видео, размещенного на своем сайте, производит их проверку.
- Организуют процесс модерации на основе результатов отчетов от сообщества пользователей, оперативные ответы на отчеты, поступившие более чем от одного пользователя и от постоянных пользователей, которые определяются по их уровню активности, или рейтинга, или репутации, полученных от других пользователей, могут помочь создать активное сообщество, которое "самостоятельно контролируется"и стремится сохранить свою и чужую онлайновую безопасность.
- Предоставляют механизм для отправления отчетов о недопустимом содержании, контактах или поведении, как указывается в их условиях обслуживания, применимых правилах использования и/или Руководствах для пользователя. Эти механизмы должны всегда быть легкодоступны для пользователей, а процедуры должны быть легко понятны и соответствовать возрасту. Отчеты должны сразу же рассматриваться, а реакция должна быть на них незамедлительной. Пользователям должна предоставляться информация, необходимая им для составления эффективного отчета, и, где возможно, должно даваться указание на то, как обычно обрабатываются отчеты.
- Связать отчеты о злоупотреблении с процессами "Предупреждения и отключения"с соглашением об уровне общественных услуг о времени ответа или отключения.
- Избегать опасного или недопустимого **рекламного содержания он-лайн**.

Ограничение доступа:

Задача ограничения доступа к недопустимому контенту может быть решена следующими способами:

- **Программное обеспечение для родительского контроля**, которое позволяет родителям управлять доступом их детей к ресурсам интернета.
- **Инструменты для более безопасной работы в интернете**, включая родительский контроль, в идеале позволят ввести следующие типы категорий: белые списки, фильтры контента, наблюдение за использованием, управление контактами, временные/программные ограничения.
- Поставка новых компьютеров или доступа к услугам интернета с **программным обеспечением для родительского контроля, активированным**

"по умолчанию", связанным с заметными сообщениями о безопасности, которые объясняют, что делают установки по умолчанию.

- **Принятие "безопасного поиска"**: большинство поисковых систем предлагают возможности безопасного поиска, которые не показывают результаты, содержащие изображения или ключевые слова, которые могут рассматриваться, как неподходящие для детей.
- Принятие соответствующих методов подтверждения возраста, чтобы предотвратить доступ детей к содержанию, сайтам, или интерактивным услугам, непригодным для данного возраста, например, чаты и т. п., где есть риск неподобающего контакта или поведения.
- **Система обозначений для контента**: Профессиональные поставщики контента, т. е. игр, редактируемого радиовещательного контента, должны обеспечивать ясное внешнее обозначение содержания их сайтов, которое показывает его доступность для детей.
- **Блокирование на уровне сети**, где на основе национальных критериев некоторые материалы из интернета, например, изображения с сексуальным насилием над детьми, признаются определенно незаконными.

Повышение устойчивости:

Повышение устойчивости детей в ситуациях, связанных с риском, является важной задачей, она взаимозависит от двух других целей снижения доступности и запрета доступа и дополняет их.

Хотя родители и дети играют свои роли в деле снижения доступности опасного и недопустимого материала, например, сообщая о злоупотреблениях поставщику услуг хостинга для сайтов, эта задача, главным образом, лежит на плечах отрасли. И хотя отрасль выполняет свою роль в создании устойчивости детей, например, предоставляя советы по обеспечению безопасности, родители и другие взрослые, работающие с детьми, вероятно имеют самое большое влияние в этой области и потому несут больше ответственности.

Такие схожие, но различные роли отрасли и семей в выполнении этих трех задач очень важны и предполагается, что необходима общая государственная стратегия, направленная на обеспечение безопасности детей в онлайновой среде, которая способна оказывать влияние и поддержку как отрасли, так и семьям.

Рассматривая сильные и слабые стороны существующих мер повышения безопасности детей в интернете и учитывая различные существующие национальные законы, отрасль интернета может разработать саморегулирующиеся национальные кодексы отраслевой практики; эти кодексы были бы более прозрачными, чем руководящие указания по передовому опыту, учитывая, что орган, который контролирует/координирует их выполнение, осуществляет эффективный контроль и публикует его результаты. Кроме того, в этих рамках могут быть разработаны механизмы, которые дают право голоса родителям и детям.

Операторы подвижной связи

Так как растущее количество операторов подвижной связи предлагает своим пользователям доступ

Ситуационное исследование: Правила безопасности "Большой Шестерки"для служб социальных сетей

- **Проверка изображений и видео:** сайты должны найти способы проверять размещаемые на них изображения и видеоматериалы и, в случае обнаружения неподобающего контента, удалять его.

- **Проверка дискуссионных групп:** сайты социальных сетей должны проверять дискуссионные группы с целью выявления опасных тем для обсуждения, агрессивных высказываний и противоправного поведения и, в случае обнаружения такого контента, удалять его.

- **Удаление зарегистрированных пользователей, совершивших преступление на сексуальной почве:** сайты социальных сетей не должны позволять лицам, совершившим преступление на сексуальной почве, создавать учетные записи на своих сайтах при помощи существующей в настоящее время технологии.

- **Значительные усилия по укреплению требований к минимальному возрасту:** сайты должны укреплять свои требования к минимальному возрасту и предпринимать шаги по определению и удалению учетных записей несовершеннолетних пользователей, которые для получения доступа неверно указали свой возраст.

- **Защита юных пользователей от нежелательного общения:** сайты социальных сетей должны по умолчанию реализовать установки обеспечения безопасности, которые мешают взрослым вступать в контакт с подростками моложе 16 лет, с которыми они не знакомы в реальном мире.

- **Сотрудничество с органами охраны правопорядка:** все сайты должны иметь доступные горячие линии связи с органами охраны правопорядка, чтобы помогать им во время экстренных и обычных расследований.

к широкому и привлекательному спектру услуг поставки контента, включая игры, музыку, видео и телепрограммы, им требуется решить задачу управления доступом пользователей к коммерческому контенту, который может быть предметом запрета повозрасту, если доступ получен при помощи разных каналов.

Все больше новых социальных и интерактивных услуг, доступных для пользователя, также сталкивается с проблемами возраста пользователей. Например, многие основные сайты социальных сетей устанавливают требования к минимальному возрасту, которые указаны в их Условиях обслуживания, так как существует мнение, что юные пользователи сталкиваются с рисками, например, кража идентичности или недопустимые контакты, связанными с размещением слишком подробной информации о себе и т. п.

Для обеспечения общего и прозрачного подхода, в некоторых странах операторы подвижной связи и поставщики контента решают эту задачу в ходе совместной работы по согласованию систем классификации. Эти системы классификации обычно создаются для управления коммерческим мобильным контентом, т. е. контентом, который операторы подвижной связи создают сами или вместе с третьими лицами, они основаны на утвержденных национальных стандартах и сочетаются с подходами, предпринимаемыми в аналогичных средствах информации, например, в играх, фильмах.

На самом деле, там, где это возможно, должна использоваться классификация контента, принятая в других отраслях. Примером может быть фильм или трейлер фильма, или компьютерная игра, учитывая, что их изображения повторяются в версиях, адаптированных для подвижного применения, так чтобы во всех национальных средствах информации одно и то же содержание было бы одинаково классифицировано для потребителя.

Однако учитывая стоящие перед операторами подвижной связи практические задачи по установлению возраста конечного пользователя, на некоторых рынках, например, в Австралии, Дании, Новой Зеландии, в настоящее время используется простая двухуровневая система классификации: содержание, подходящее только для взрослых, и другое/общее содержание.

Например, австралийский кодекс просто отображает все существующие критерии и уровни, определяемые Классификационной комиссией, как "запрещенные" для взрослых старше 18 лет, и "незапрещенные" (для всех), которые используются на рынке подвижной связи, тогда как операторы в США, под покровительством своего профсоюза CTIA, создали сетку, которая относит существующие стандарты, принятые для телевидения, фильмов, музыки и игр, либо к категории "Доступно с применением сотовой связи" (общая категория), либо к категории "Запрещено для доступа с применением сотовой связи" (старше 18 лет), результаты этого CTIA излагает следующим образом.

Этот двоичный подход позволяет операторам подвижной связи и третьим лицам продавать широкий спектр легального коммерческого контента, который соответствует национальным испытаниям на приемлемость; он гарантирует контролируемость в области самого большого риска, а также отражает тот факт, что совершеннолетие является наиболее практичной точкой проверки по возрастам, например, проверяя достижения возраста для участия в выборах или возраста владения кредитной картой.

Однако на некоторых рынках происходит движение в сторону более детального подхода. В Германии принята трехуровневая система классификации коммерческого

Ситуационное исследование: Критерии классификации руководящих указаний для беспроводного доступа к контенту в США

контента, которая в общих чертах основана на системе классификации фильмов в Германии "FSK":

- Общий контент /услуги: доступные всем по умолчанию.
- Контент /услуги: для лиц старше 16 лет – доступны всем по умолчанию, родители могут принять решение о применении блокировки.
- Контент /услуги: для лиц до 18 лет – по умолчанию заблокированы для всех пользователей, взрослые должны пройти процедуру проверки возраста.

Во Франции рекомендованная четырехуровневая система классификации ("все пользователи", до 12 лет, до 16 лет, до 18 лет), созданная в процессе консультаций с большим числом заинтересованных сторон при поддержке Форума Le Forum des droits sur l'Internet, была введена в октябре 2006 года. Четыре разных уровня облегчат

Контент, доступный в сети подвижной связи, будет классифицироваться как "контент, ограниченный для доступа в сети подвижной связи"или "контент, доступный для всех в сети подвижной связи"на основе существующих критериев, используемых для присвоения категорий фильмам, телевизионным программам, музыке и играм.

Контент, как правило, считается "ограниченным", если он содержит любой из указанных ниже идентификаторов запрещенного содержания:

Контент, ограниченный для доступа в сети подвижной связи:

- Нецензурная лексика;
- Повышенная жестокость;
- Графическое изображение сексуальной активности или сексуальных сцен > обнажение;
- Агрессивная лексика;
- Графическое изображение употребления нелегальных наркотиков;
- Любые действия, запрещенные законом для лиц старше 18 лет, например, азартные игры и лотереи.

Любой контент, не отнесенный к группе "контент, ограниченный для доступа в сети подвижной связи ", будет считаться "контентом, доступным для всех в сети подвижной связи " и будет доступен всем потребителям.

Более подробно о Руководящих указаниях для беспроводного доступа к контенту можно найти на веб-сайте CTIA: http://www.ctia.org/advocacy/index.cfm/AID/10394

борьбу с проблемами, связанными с управлением доступом к интерактивным услугам и контенту, созданному пользователем, большая часть которого подходит для старших подростков, а не с контентом "только для взрослых" или для младших подростков и детей.

Для получения доступа к контенту, имеющему отметку "старше 18 лет", пользователи должны пройти процедуру проверки возраста; отметки "старше 12 лет" и "старше 16 лет" будут соответствовать двум следующим уровням родительского контроля:

- Отметка "Родительский контроль первого уровня" (Contrôle parental de premier niveau): блокирует доступ к коммерческому контенту с отметкой "старше 16 лет", созданным пользователем/интерактивным услугам, которые помогают встретиться, например, сайтам знакомств, интернету.
- Отметка "Усиленный родительский контроль" (Contrôle parental renforcé): блокирует доступ к контенту с отметкой "старше 12 лет" и "старше 16 лет", ко всем созданным пользователем/ интерактивным службам, интернету.

Системы классификации контента либо создаются самим оператором сообщества, либо заимствуются у третьего лица, обладающего соответствующей квалификацией. Многие страны, включая, например, Данию, Малайзию, Сингапур и Новую Зеландию, просто обозначили рамки классификации в рамках своего национального кодекса отраслевой практики или как дополнение к нему.

Другие страны, включая упомянутую Францию, используют критерии классификации, созданные третьей организацией. Двухуровневая система в Соединенном Королевстве была запущена Независимой отраслевой организацией по классификации подвижного контента (IMCB: http://www.imcb.org.uk/) в 2005 году. Кроме формулировки критериев классификации, IMCB может дать совет или выступить в роли арбитра в (очень редких) спорах по классификации отдельных элементов контента.

Следует заметить, что не все системы классификации контента строятся на основе определения возраста: в Малайзии и Сингапуре используется двоичная система классификации содержания на основе существующих национальных стандартов, однако она основана на противопоставлении "приемлемого" и "неприемлемого" контента и не имеет различий, основанных на возрасте.

Совместное применение систем классификации упрощает самоклассификацию для партнеров в области контента и, тем самым, уменьшает затраты и повышает эффективность отрасли в целом. Кроме того, при этом система классификации становится более прозрачной для потребителя, особенно для независимых услуг, предоставляемых третьей стороной на портале оператора, например, в журналах, и это позволяет осуществить последовательное введение таких инструментов, как заранее назначенные короткие шифры "взрослого содержания" для специальных услуг СМС, которые могут облегчить реализацию контроля возраста.

3. Механизмы управления контентом

Поставщики онлайнового контента и услуг разрабатывают ряд подходов для предоставления возможности управления контентом в онлайновой среде в соответствии с возрастными рамками. Такие подходы включают механизмы, которые ограничивают доступ к контенту до тех пор, пока пользователь не доказал свой возраст ("подтверждение возраста"), а также предоставляет родителям функции контроля, с тем чтобы они имели возможность ограничить потребление своим ребенком онлайнового контента и услуг.

Радиовещательные организации

Радиовещательные организации часто предлагают большой выбор онлайнового контента и услуг, в том числе, предназначенного только для пользователей старше определенного минимального возраста. Для гарантии того, что младшие пользователи получают только контент, соответствующий их возрасту, радиовещательные организации используют ряд методов, таких как:

- Процессы однократной регистрации. Например, в онлайновых службах BBC, когда дети регистрируются на форумах, их просят сообщить дату рождения. Эта информация

Примечание 1. – Механизмы для борьбы с незаконным онлайновым контентом, в частности, с материалами, содержащими сексуальное насилие над детьми, рассматриваются отдельно в следующем разделе.

Примечание 2. – Более подробная информация относительно радиовещательных организаций и контента, создаваемого пользователем, можно найти в разделе 6.

затем используется для определения того, достаточно ли они взрослые, чтобы получить доступ к услугам, причем позже дети не могут изменить исходную дату рождения, если они обнаруживали, что определенное содержание им не доступно в силу их возраста.

- Согласие родителей, полученное по электронной почте. Например, BBC в настоящее время участвует в целом ряде испытаний, с целью пересмотра использования согласия родителей по электронной почте и создания системы регистрации, которая позволила бы родителям решать, какие действия могут совершать их дети на веб-сайтах PSB и какой уровень отчетов они будут получать. BBC также рассматривает вопрос том, какие правила должны применяться для подростков до 16 лет и должны ли они иметь доступ к более высоким уровням обмена данными прежде, чем они будут должны спросить получить согласие родителей.
- Сегодня многие государственные радиовещательные организации, ожидая лучшего регулирования[4], применяют к веб-решениям более решительный подход, чем к своему эфирному вещанию. RAI, Италия, например, использует политику ограничения и не размещает на своих веб-сайтах какой-либо контент, который не был бы отнесен к группе "разрешен для всей семьи" (обозначаемое белой бабочкой). Весь контент, обозначенный желтой бабочкой (для просмотра только с взрослыми) или красной бабочкой (только для взрослых) в настоящее время не доступен в интернете.

Поставщики услуг интернета

Важно, чтобы поставщики услуг интернета предлагали средства контроля, которые предотвращают доступ к определенным типам контента и услуг.

Во многих странах национальный закон указывает, что некоторые типы контента или услуг не должны быть доступны детям, т. е. тем пользователям, которые не достигли установленного законом возраста совершеннолетия/взрослости. Там, где услуги предоставления такого контента предлагаются поставщиками услуг интернета на коммерческих условиях, должен использоваться механизм подтверждения статуса взрослого. Либо, если закон не требует этого, может применяться общепринятый расчет на то, что дети и молодые люди не должны иметь доступ к контенту, предназначенному только для взрослых. В этой связи поставщики услуг интернета и других услуг возможно захотят рассмотреть вопрос о создании или использовании систем с возрастными рамками в качестве средства обеспечения соблюдения законодательных норм.

Поставщики услуг интернета должны иметь в виду, что простые клики для подтверждения возраста, которые используются, для того чтобы пользователь подтвердил, что ему больше 18 лет, не надежны, потому что они полностью полагаются только на честность пользователя.

[4] Стоит отметить, что BBC выразила некоторые предостережения в том, как позволить пользователям активировать "красную кнопку", если они сталкиваются с материалом, который является вредным, недвусмысленным или беспокоит их. Основной проблемой является то, что при наличии большого числа опций, это может увести пользователей на другие, менее заслуживающих доверия, неконтролируемые сайты. Важно, чтобы поставщики услуг интернета сохранили свою репутацию в том, что они предоставляют безопасные условия и тем самым гарантируют, что не будут возникать опасения о критическом нарушении безопасности.


“Отрасль выполняет обязательства по разработке ответственного подхода к проблемам детей, использующих онлайновые услуги связи и ИКТ”

Однако, важно также знать, что даже решения, которые стремятся определить возраст пользователя, например, требуя номер кредитной карты или паспортные данные, не могут полностью гарантировать достоверность: главными проблемами для всех методов подтверждения возраста является то, что идентифицировать личность в интернете сложно, потому что фактически невозможно знать, является ли отдельный пользователь, предоставляющий информацию, действительно тем человеком, данные о котором он предоставил. Хотя пользователь может предоставить определенную информацию при регистрации на веб-сайте, не существует действенного или эффективного способа проверить правдивость введенной им информации. Например, для определения возраста человека не всегда можно полагаться на применение выпущенных правительством национальных ID-карты с PIN-кодом, так как детали данных часто известны другим, например, членам семьи.

Такие подходы могут также потенциально нарушать права пользователя на неприкосновенность частной жизни, например, ID-карты раскрывают персональные данные, такие как дату рождения, не считая тех данных, которые являются абсолютно необходимыми для подтверждения того, что пользователь достиг совершеннолетия.

Поставщики услуг интернета становятся все более изобретательными в решении проблем, связанных с контентом, доступ к которому ограничен возрастными рамками. Например, услуга MySpace в своих Условиях использования требует, чтобы все пользователи были в возрасте 13 лет или старше, а для того чтобы бороться с ситуацией, когда пользователь в возрасте до 13 лет лжет о своем возрасте, применяется алгоритм поиска, который ищет такие слова, которые часто используются несовершеннолетними пользователями, находит и удаляет профиль несовершеннолетнего ребенка. Сайт MySpace проверяет наличие таких терминов и обновляет поисковые базы данных с учетом изменений в поведении пользователей и терминологии.

Многие крупные поставщики услуг интернета в настоящее время предлагают решения для родительского контроля, которые помогают родителям контролировать к каким сайтам, контенту и услугам разрешить получить доступ своим детям.

Ситуационное исследование: Telecom Italia и защита детей – Италия

Для того чтобы обеспечить детям и подросткам безопасную работу в интернете, Telecom Italia предприняла определенные шаги, для того чтобы запретить контент нарушающий психофизическую целостность ребенка, описанную на портале Группы[5], и предоставила своим потребителям защищенные услуги и инструменты, способствующие безопасной работе в интернете[6].

Важнейшим инструментом для детей является программное обеспечение **Alice's Magic Desktop**, которое является упрощенной операционной системой, работающей на обычных ПК. Alice's Magic Desktop позволяет детям безопасно использовать ПК и разрешенные занимательные и обучающие функциональные возможности интернета под бдительным контролем родителей. Целевой аудиторией этой услуги являются дети 10 лет и младше.

Основные характеристики продукта:

- **Защита ПК** от неправильного использования детьми во избежание повреждения оборудования, конфигурации, установленного программного обеспечения родителей и т. д.;
- **Безопасная работа в интернете** на основании предоставленного родителями белого списка предпочитаемых веб-сайтов;
- Специальный детский **клиент электронной почты** со специализированным графическим интерфейсом пользователя и предварительно составленной родителем адресной книгой;
- **Онлайновые игры и инструменты** для изучения и использования множества познавательных материалов;
- **Интерфейс полного родительского контроля**, который позволяет родителям контролировать и определять "защищенную область"для детей.

Детям очень просто существовать в этой безопасной среде, где имеются различные темы для рабочего стола и персонализированным интернет-браузером ("Мой первый браузер"), где ребенок может посещать только "предпочтительные"сайты, одобренные родителями; с почтовой программой Magic email, которая не позволяет получать электронную почту с недопустимого адреса, и прежде, чем доставить письмо ребенку, оно для проверки родителем помещается в папку "карантин".

Источник: Telecom Italia

Кроме того, Telecom Italia для выполнения строгих ограничений национального Закона Италии о защите детей[7], а также обеспечения реагирования на проблемы защиты и безопасности граждан, которые используют коммерческие услуги, приступила к реализации программы тесного сотрудничества с итальянской полицией и со специализированным Национальным центром по борьбе с детской порнографией в онлайновой среде (CNCPO)[8], создавая при этом узкоспециализированную технологическую инфраструктуру доступа и реализовывая систему фильтрации, блокирующую сайты, указанные центром CNCPO.

[5] www.telecomitalia.com, Sustainability->Hot Topics-> Protection of Children and Abuse

[6] Alice Total Security and Alice Magic Desktop, http://adsl.alice.it/servizi/index.html

Кроме того, для борьбы и предотвращения распространения контента с сексуальным насилием над детьми (детской порнографии) и защиты детей, Telecom Italia создала веб-механизм помощи/доверия, позволяющий сообщить на веб-сайте о незаконном контенте, с которым сталкиваются пользователи, работая в интернете. Эти сообщения, которые могут быть написаны анонимно путем заполнения стандартной онлайновой формы, анализируются и незамедлительно отправляются Почтовой полиции (CNCPO), которая будет расследовать предполагаемые преступления, так как данный тип деятельности поручен исключительно полиции.

Несмотря на то, что решения для родительского контроля все время совершенствуются, они, как ожидается, не обеспечат полную безопасность, однако, в связи с тем, что интернет используется для обучения детей (смотри "Обучение и общение с пользователем", ниже), родительский контроль может помочь младшим пользователям получить опыт безопасной работы в онлайновой среде.

Операторы подвижной связи

Механизмы контроля доступа контенту с ограничениями по возрасту, разбиваются на две большие категории:

- Механизмы подтверждения возраста;
- Родительский контроль.

Механизмы подтверждения возраста

Инструменты "проверки возраста", доступные традиционным розничным торговцам мультимедийной информацией и контентом, а также радиовещательным организациям, не могут просто переноситься в мобильную среду передачи контента. Например, в случае мобильного контента нет возможности осуществить визуальную проверку в "пункте продажи", возможную в кинотеатрах и магазинах; и учитывая персональный характер мобильного устройства, операторы подвижной связи не могут надеяться на родительский контроль в той же степени, в какой традиционно могли это делать радиовещательные организации ТВ.

Однако ряд операторов по всему миру решают эту задачу путем разработки систем подтверждения возраста. На сегодняшний день, как правило, они требуют подтверждения возраста от взрослых, желающих получить полный доступ ко всему контенту и услугам. Следует отметить, что это имеет особое значение там, где операторы предлагают коммерческие услуги и контент, которые подлежат возрастному ограничению в соответствии с законодательством.

---

[7] Итальянский Закон № 38/2006 борется с сексуальной эксплуатацией детей и детской порнографией, в том числе посредством интернета; законодательный акт Италии № 70/2003, который регулирует электронную торговлю и требует от операторов телефонной связи, таких как Telecom Italia, предоставлять в компетентные органы отчеты о киберпреступлениях, связанных с инфраструктурой сети и замеченным случаях сексуального насилия над ребенком; Конвенция по киберпреступности ЕС, подписанная Советом Европы 23 ноября 2001 года, ратифицирована в Италии Законом № 48/2008.

[8] http://www.poliziadistato.it/articolo/10232-Centro_nazionale_per_il_contrasto_alla_pedopornografia_sulla_rete

Различные операторы применяют различные подходы для подтверждения возраста, основанные на применении существующих вариантов, таких как:

- Схемы с использованием государственных ID;
- Кредитные карты;
- Номера налогоплательщиков;
- Списки избирателей;
- Личная проверка ID в магазине или, например, в почтовых отделениях;
- Статус контракта/существующая взаимосвязь с плательщиком.

После подтверждения возраста взрослого пользователю либо выдают "PIN-код только для взрослых", который должен вводиться каждый раз, когда пользователь желает получить доступ к контенту и услугам, предназначенным только для взрослых, либо учетная запись пользователя получает статус профиля взрослого, и снимаются любые ограничения на контент и услуги.

Из-за трудностей, связанных с подтверждением достижения возраста совершеннолетия в виртуальной/"онлайновой" среде, операторы дают возможность родителям контролировать доступ младших пользователей к контенту и услугам при помощи родительского контроля, вместо того чтобы подтверждать возраст каждого конечного пользователя.

Родительский контроль

В то время как механизмы подтверждения возраста означают, что операторы заранее создают системы, которые гарантируют доступ к определенному контенту индивидуальным потребителям, достигшим определенного возраста, средства родительского контроля полагаются на инициативу и использование родителями такого контроля, какой они считают необходимым для своего ребенка.

Многие операторы из ряда стран уже ввели системы родительского контроля, некоторые из них нацелены только на блокирование доступа к коммерческому контенту, несоответствующему возрасту, другие объединяют его с дополнительными функциями, такими как контроль времени или потраченных средств.

За некоторыми исключениями, включая операторов во Франции, которые уже создали два уровня доступа, а также нескольких других операторов по всему миру, которые разработали различные многоуровневые системы родительского контроля, в большинстве систем, как правило, используются параметры "включить" или "выключить", при включении которых блокируется доступ на определенный уровень для получения коммерческого контента и услуг, с ограничениями по возрасту, например, 18 или 16 лет.

Большинство систем родительского контроля в настоящее время обращают внимание исключительно на коммерческий контент, поскольку в этой области оператор имеет наибольшую степень контроля и, следовательно, ответственности. Операторы в Японии используют в качестве подхода систему черных/белых списков для веб-сайтов, когда применяется родительский контроль, и некоторые операторы на других рынках применяют системы интернет-фильтрации, но большинство операторов еще только должны ввести интернет-фильтрацию, как часть своих услуг в сфере обеспечения родительского контроля.

В качестве временной меры ряд операторов просто блокируют доступ в интернет, когда включен родительский контроль.

Вероятно однако, что растущая тенденция к использованию мобильных телефонов для доступа к интернет-услугам позволит ускорить развертывание инструментов интернет-фильтрации.

Обычно, учитывая, что ответственность несут родители или опекуны, применяющие контроль, ключевым моментом для повышения общей эффективности этой возможности для защиты младших пользователей является продвижение данного варианта и повышение осведомленности о нем. Кроме того, операторы должны убедиться, что родители понимают, что они могут контролировать только контент, который доставляется по их собственным сетям.

Другие варианты для рассмотрения включают установку операторами подвижной связи систем родительского контроля на фирменных телефонах по умолчанию и, возможно, размещение производителями мобильных телефонов программного обеспечения, которое дает родителям возможность контролировать использование и ограничивать список тех, кто может связаться с их ребенком.

Ситуационное исследование: Родительский контроль в сети ATT MEdia™ – США

Услуга родительского контроля AT&T предоставляется потребителям бесплатно. Она позволяет родителям ограничить доступ их детей через мобильный телефон к контенту для взрослых, а также предлагает функцию запрета на покупку загружаемых файлов, таких как игры и рингтоны.

Контролируемый контент: родители могут включить фильтры контента, используя опции "включить" или "выключить". Если фильтр контента "включен", доступ к контенту для взрослых на портале AT&T MEdia™ (например, чат, знакомства) ограничен, а доступ к более широкому мобильному интернету с помощью функции поиска отключен. Если фильтр "выключен", то ограничений нет, и весь контент виден и доступен. Фильтр контента по умолчанию установлен в положение "выключен".

Ситуационное исследование: Родительский контроль в сети NTT DocoMo – Япония

DoCoMo предлагает различные уровни фильтрации контента (например, режим фильтрации при работе в интернете "Дети"и режим фильтрации при работе в интернете), плюс опцию "ограничение по времени", которая может использоваться самостоятельно или вместе с другими уровнями фильтрации контента. Все три варианта предлагаются потребителям бесплатно:

1. Режим фильтрации при работе в интернете "Дети": позволяет получить доступ только к тем сайтам, которые находятся в меню режима работы в интернете (поставщики услуг интернета в меню режима работы в интернете по договору запрещают предложения "вредного контента", включая контент для взрослых и контент с возрастными ограничениями, азартные игры, насилие, службы знакомств, чаты и форумы); "Детское меню в интернете"состоит из сайтов, специально разработанных для детей, которые устанавливаются в меню по умолчанию.
2. Режим фильтрации при работе в интернете: позволяет получить доступ только к тем сайтам, которые находятся в меню режима работы в интернете, а также независимым сайтам, которые не содержат вредоносного контента.
3. Ограничение по времени: запрещает доступ к любому сайту (будь то первый режим или второй) между 22.00 и 06.00.

4.

Обучение и общение с пользователем

Для того чтобы позволить пользователям принимать обоснованные решения относительно контента и услуг, которые они хотят использовать, а также дать родителям и учителям возможность указывать детям и подросткам направление к получению безопасного, надежного и надлежащего опыта в онлайновой среде, поставщики услуг электросвязи и контента все больше и больше инвестируют в обучающие программы и общение.

Этот раздел описывает ряд возможных подходов, осуществляемых поставщиками услуг интернета для предоставления онлайнового контента и услуг.

Радиовещательные организации

Радиовещательные организации, которые создают программы, пользующиеся популярностью у детей и младших пользователей, вероятно, будут иметь соответствующую юную "аудиторию" в онлайновой среде и, следовательно, будут нести особую ответственность за поддержание безопасности в онлайновой среде.

Радиовещательные организации также имеют хорошие возможности, для того чтобы пользоваться популярность своего содержания с целью доставки простых сообщений, помогающих младшим пользователям противостоять таким ситуациям, как "кибер-запугивание" или вторжение в частную жизнь.

Другие подходы, которые могут быть предприняты радиовещательными организациями, включают в себя поощрение детей к получению согласия родителей, прежде чем использовать конкретные виды услуг. При создании учетной записи пользователя детям можно посоветовать спросить разрешения родителей и удостовериться в том, что их родители знают о том, что они будут использовать такие услуги, как форумы. В Условиях использования можно также указать, что дети должны иметь разрешение родителей или опекуна, прежде чем общаться на форумах.

Если ребенок разместил сообщение, которое наводит на мысль о том, что его родители не знают или не хотят, чтобы он использовал услуги общения радиовещательных организаций, то обычно веб-мастер направит пользователю сообщение, разъясняя, что для пользования форумом он должен иметь разрешение родителя/опекуна.

Некоторые организации для дополнительной безопасности требуют подтверждения от родителей в виде ответа на письмо электронной почты. Однако, например, опыт компании BBC по тестированию собственных пользователей показывает, что многие дети используют адреса электронной почты своих родителей, это может подорвать эффективность системы, и что часть аудитории BBC имеет доступ к CBBC только из групп продленного дня, либо потому что они не получают должной поддержки дома, либо потому что они не имеют доступа к интернету.

Таким образом, решение в виде постановки галочки в нужный квадратик или в виде подтверждения по электронной почте не являются достаточными, для того чтобы признать, что информированный родитель/опекун/учитель фактически наблюдает за деятельностью ребенка, и этого очень мало для того, чтобы помочь тем детям, которые оказались по другую сторону цифрового разрыва. В данной области необходимо провести общеотраслевые исследования с целью отыскания более надежных процедур получения согласия родителей, которые учитывали бы удобны для населения и не допускали бы злоупотреблений.

Поставщики услуг интернета

Отрасль интернета обязана пересмотреть роль и значение взаимодействия с пользователями в области:

- **Ясности** о природе содержания, условиях использования (T&C) и политике допустимого использования (AUP);
- **Повышения осведомленности** при помощи определенных веб-сайтов, посвященных интернет-угрозам и доступным инструментам для защиты детей;
- **Совместной деятельности**, при помощи форм онлайновых отчетов;
- **Информации** для родителей и учителей о безопасности ребенка в онлайновой среде;
- **Обучения** детей безопасному использованию интернета.

Каждая из этих областей подробно рассматривается ниже.

Ясность *о природе содержания, условий использования и политике допустимого использования*:

Поставщики услуг интернета все чаще признают, что важно ясно объяснить, какова природа контента и услуг так, чтобы все пользователи, включая самых младших, могли принять обоснованное решение об их использовании.

Ясность для отрасли интернета означает:

- Установку специальных знаков для содержания, предназначенного только для взрослых;
- Сообщение о цене контента, условий подписки, способа отмены подписки и так далее;
- Определение и сообщение ясной политики допустимого использования, условий использования;
- Определение и обновление политики, которая соответствует всем соответствующим национальным кодексам по безопасному использованию интернета младшими пользователями и детьми.

Повышение осведомленности *при помощи определенных веб-сайтов, посвященных интернет-угрозам и доступным инструментам для защиты детей*:

Поставщики услуг интернета могут способствовать повышению осведомленности в вопросах защиты детей, показывая на своем сайте ясную информацию о безопасном использовании интернета и об инструментах для защиты детей. Данная специфическая область в сети должны быть предназначена, для того чтобы:

- Содействовать повышению осведомленности и обсуждению в сфере интернет угроз и защиты детей, а также инструментов, доступных для их защиты, таких как блокирование и настройка конфигурации;
- Давать пользователям советы по безопасности в онлайновом режиме;
- Содержать обучающие ресурсы;
- Описать государственную и международную нормативно-правовую базу;
- Предоставить потребителю информацию об имеющихся инструментах для защиты детей (родительский контроль и т. д.).

Совместная деятельность *при помощи форм онлайновых отчетов*:

В целях пресечения и предотвращения использования контента,

содержащего сексуальное насилие над детьми и для защиты детей, поставщики услуг интернета должны:

- Предоставить пространство в сети, доступное для написания отчетов о незаконном содержании, с которым сталкиваются пользователи при работе в интернете; такие отчеты могут отправляться анонимно посредством заполнения стандартной формы;
- Предоставлять пользователям подробную информацию о том, как сообщать о проблемах безопасности;
- Немедленно связаться с соответствующими органами полиции/охраны правопорядка, которые будут расследовать предполагаемые преступления; персонал поставщиков услуг интернета, следящий за предоставлением услуг потребителям, должен иметь средства для обработки и передачи отчетов потребителей соответствующим органам.

Информация *для родителей и учителей*:

Поставщики услуг осознают, что очень важно предоставить родителям и учителям необходимую информацию, дающую им возможность понять, как их дети используют услуги ИКТ, включая такие вопросы, например, как запугивание, и хорошо ориентироваться, чтобы указывать детям направление правильного использования.

- Для того чтобы лучше защитить своих детей, родители и учителя должны быть осведомлены о рисках в интернете.
- Эта информация должна передаваться по множеству мультимедийных каналов, так как многие родители не пользуются услугами интернета. Например, в процессе сотрудничества с районными школами для предоставления программы безопасности в онлайновой среде и обучающих материалов для родителей. Там, где это возможно, поставщики услуг интернета должны также рассказывать о государственных службах поддержки, куда родители и опекуны могут сообщить о случаях насилия и эксплуатации и получить поддержку.

Родители и учителя должны:

- Заниматься самообучением относительно использования интернета и способов, используемых их детьми для доступа к нему, а также технологии в целом;
- Изучить и оценить эффективность доступных технологических инструментов для своего ребенком и всей семьи, и выбрать те инструменты, которые могут потребоваться;
- Принимать участие и интересоваться тем, как используется интернет их детьми;
- Осознавать общие риски для молодежи, чтобы помочь своим детям понять и ориентироваться в технологиях;
- Быть внимательными к поведению детей из группы риска в их сообществе и к группе сверстников своих детей;
- Понимать, когда им необходимо обратиться за помощью к другим.

Обучение *детей безопасному использованию интернета*:

Для "маленьких навигаторов" виртуальный мир являются полезным и забавным ресурсом, но он также является и тем местом, где они могут получить доступ к материалам, которые не подходят для них.

Использование детьми интернета варьируется в зависимости от их

возраста и уровня развития, самые младшие пользователи не в состоянии самостоятельно понять преимущества и опасности интернета, поэтому предпочтительно, чтобы их во всех случаях сопровождали взрослые (родитель и/или учитель), которые могут помочь и направить их при выборе содержания, а также помочь установить соответствующие правила поведения, которым они должны следовать.

Для подростков, однако, задача труднее. Они более независимы и больше знают о возможностях, предлагаемых в интернете, часто знают гораздо больше, чем их родители и учителя о программном обеспечении для интернета, мгновенном обмене сообщениями, чатах и онлайновых играх и т. д. Тем не менее, хорошей идеей для родителей является создание правил, а также обучение их бдительности, хорошим манерам и ответственности, когда они проводят время в интернете.

Также очень важно, чтобы поставщики услуг интернета предоставляли информацию по безопасному использованию интернета напрямую детям. Дети должны получать знания о том, как выявлять и как реагировать на неправильное поведение. Ниже предлагается список советов для самоконтроля, который поставщики услуг интернета могут предоставлять своим младшим пользователям:

- "Никогда не давай контактную информацию";
- "Никогда не соглашайся на встречу с любым лицом, которого ты встретил в интернете, особенно без предварительной консультации со взрослым";
- "Не отвечай на несоответствующие (запугивающие, непристойные или оскорбительные) сообщения и сохрани доказательство, не удаляй его";

- "Расскажи взрослому, если ты испытываешь тревогу или расстроен из-за чего-то или кого-то";
- "Никогда не разглашай свой пароль к учетной записи или имя пользователя; и знай, что другие игроки могут давать ложную информацию о том, кто они в реальном мире".

Там, где это возможно, поставщики услуг интернета, должны также рассказывать о государственных службах поддержки, куда дети могут сообщить о случаях насилия и эксплуатации и получить поддержку.

Применение Условий использования

Очень важно, чтобы поставщики услуг интернета и отрасль интернета в целом помещали на первый план "страницу Условия использования"(T&C) на сайтах услуг, предоставляе мых в интернете, с ясным описанием политики санкций за нарушение Условий использования. Например, типичные положения страницы "Условия использования"отмечают, что потребитель не должен использовать веб-сайт или услугу для того, чтобы:

- Загружать, публиковать, передавать, совместно использовать, хранить или распространять любой контент, который может быть вредным, незаконным, клеветническим, нарушающим права, оскорбительным, вульгарным, непристойным, нарушающим конфиденциальность или общественные права, содержащим выражения ненависти или расизм;
- Выдавать себя за другое физическое или юридическое лицо, или указывать ложный возраст, принадлежность к любому физическому или юридическому лицу;
- Загружать, публиковать, передавать, совместно использовать, хранить, размещать на веб-сайтах любую частную информации, касающуюся третьих лиц, включая адреса, номера телефонов, адреса электронной почты, номера кредитных карт;
- Запрашивать личную информацию от лиц моложе 18 лет, включая, но, не ограничиваясь этим: имя, адрес электронной почты, домашний адрес, номер телефона или название своей школы;
- Загружать, передавать, совместно использовать любые материалы, которые содержат вирусы;
- Загружать, публиковать, передавать, совместно использовать или предоставлять контент, используя который можно будет совершить, спровоцировать уголовное преступление, нарушающие права любой стороны или любых местных, государственных или международных законов;
- Вредить или эксплуатировать детей в любой форме;
- Выслеживать, клеветать, обманывать, извещать, унижать достоинство лица или группы лиц по любой причине, в том числе по признаку возраста, пола, инвалидности, национальности, расы, религии или сексуальной ориентации.

Условия использования должны поддерживаться ясным разъяснением политики компании в отношении любых нарушений и, как правило, включают в себя такие пункты:

- [Компания X] приняла правило, по которому удаляет учетные записи тех пользователей, которые считаются злостны-

ми нарушителями. Она оставляет за собой право по своему усмотрению без предварительного уведомления просматривать и удалять созданные пользователем услуги и контент, а также удалять контент и учетные записи;

- [Компания X] также может по своему собственному усмотрению ограничивать доступ на сайты или прекращать членство любых пользователей, кто нарушает правила.

Поставщики услуг интернета должны повторить ключевые положения из своих Условий использования удобным для пользователя языком в общих руководящих указаниях и "напоминаниях", которые включены в саму услугу, например, напоминая в месте загрузки контента пользователям о том, какие виды контента считаются несоответствующими.

Операторы подвижной связи

Обучение и общение с пользователем играет ключевую роль в обеспечении того, чтобы дети и младшие пользователи могли приобрести безопасный и подходящий по возрасту опыт использования подвижной связи.

Операторы все чаще признают важность ясного указания природы содержания и предлагаемых услуг таким образом, чтобы все пользователи, включая младших пользователей, могли принимать обоснованные решения относительно их использования. Это включает установку указателей на содержание с учетом возрастной специфики, но также требует ясности общения с учетом стоимости контента, условий подписки и действий для отказа от подписки и все другое не менее важное, потому что отсутствие абсолютной ясности в данной области приводит к рискам для младших пользователей, в частности, к непреднамеренной подписке на услугу, например, когда они первоначально намеревались купить единственный рингтон.

Как и в других мультимедийных службах, операторы подвижной связи не могут нести полную ответственность за обеспече-

Ситуационное исследование: Кодекс поведения Ассоциации поставщиков услуг беспроводных приложений в отношении СМС, предоставляемых за дополнительную плату – ЮАР

Кодекс WASPA состоит из ряда обязательств, специально разработанных для ясного общения с пользователями. Примеры таких обязательств включают следующее:

- **Реклама всех услуг с абонентской платой должна указывать и четко определять эти услуги, как "услуги с абонентской платой";**
- **После того как пользователь подписался на услугу с абонентской платой, ему должно быть отправлено уведомление, содержащее следующую информацию:**

a) Стоимость подписки и периодичность платежей;

б) Четкие и краткие инструкции на случай, если пользователь захочет отказаться от подписки на услугу;

c) Контактная информация участника.

- **Подписанным пользователям необходимо ежемесячно отправлять сообщения-напоминания, содержащие информацию, перечисленную в (a, б и c, выше).**

Полный Кодекс поведения можно найти на веб-сайте WASPA http://www.waspa.org.za

Исследование: Программа Vodafone "Лучшие советы"для родителей – Соединенное Королевство

ние того, чтобы дети и подростки использовали свои мобильные устройства соответствующим образом; родители, воспитатели и педагоги тоже играют в этом свою роль. Проблема состоит в том, что родители зачастую менее осведомлены о возможностях новых мобильных устройств, чем сами дети, таким образом, ключевым фактором является обучение этой группы.

Для этого ряд операторов инвестировали разработку программ обучения и руководящих указаний, предназначенных для родителей и охватывающих полный диапазон вопросов, таких как:

- Содержание и услуги: объяснение родителям видов услуг, доступных на сегодняшний день (например, объяснить, что такое сайты общения в социальных сетях? Что такое услуги, предоставляемые с учетом местоположения пользователя? Как осуществляется доступ в интернет с мобильного телефона?) и, в соответствующих случаях имеющиеся варианты применения родительского контроля;
- Несоответствующий контакт: как избежать "большой опасности"; что делать, если ребе-

В рамках инициатив обучения детей безопасности компания Vodafone разработала высокоуровневый карманный справочник для родителей "Лучшие советы". Этот справочник содержит рекомендации по ряду областей, включая чат, игры, платные услуги и запугивание.

Следующие "Лучшие советы" касаются загрузки содержания на мобильные телефоны:

- Обсудите с вашим ребенком, какие услуги он может использовать на своих мобильных телефонах, например, он может загружать рингтоны, обои или игры напрямую со своего мобильного телефона.
- Узнайте, будет ли он использовать загруженное содержание вместе с друзьями.
- Обсудите с ребенком типы контента, потенциально неуместные, для того чтобы загружать, принимать или делиться с другими.
- Подчеркните, что не надо реагировать на любые сообщения от незнакомых людей, а также сообщения, которые смешны или предлагают дешево продавать продукты. Они "слишком хороши, чтобы быть правдой".
- Убедитесь, что любые телефоны, у которых отключен режим контроля контента, недоступны для ваших детей.
- Вы можете повторно применить режим контроля контента, позвонив в сервисную службу Vodafone по телефону 191, посетив розничные магазины Vodafone или сайт в интернете: www.vodafone.co.uk

"Оставаться на связи: Руководящие указания для родителей по использованию мобильных телефонов"Лучшие советы можно загрузить на: http://online.vodafone.co.uk/dispatch/Portal/SimpleGetFileServlet?dDocName=VD007645&revisionSelectionMethod=latestReleased&inline=0

нок подвергается запугиванию посредством так называемого "киберзапугивания" или СМС;

- Какие шаги предпринять, если телефон был украден или если ваш ребенок получает спам;
- Контроль конфиденциальности – не обмениваться информацией в онлайновой среде, хранить профили на частной SNS и т. д.

Обучая родителей, операторы дают им возможность направлять их детей к безопасному и ответственному самостоятельному использованию услуг подвижной связи. Некоторые операторы объединили свои усилия с другими участниками рынка, чтобы разрабатывать и продвигать общие руководящие указания для родителей, например, во Франции[9], Ирландии[10], тогда как другие предлагают собственные руководящие указания компании для своих частных пользователей.

Точно также повышение осведомленности о наличии инструментов родительского контроля имеет жизненно-важное значение, особенно в тех странах, где они не применяются по умолчанию. С учетом этого операторы все чаще размещают информацию о функциях родительского контроля на веб-сайтах в магазине, на корешке счета на оплату и предлагая средства родительского контроля в пунктах продажи.

Операторы также взаимодействуют с младшим пользователем непосредственно через онлайновые обучающие программы и партнерские отношения с неправительственными организациями (NGO) на местных рынках, а также косвенным образом, предоставляя учителям ресурсы, для того чтобы обучать и информировать учащихся о надлежащем использовании, смотри, например, веб-сайт "Учи сегодня" (www.teachtoday.eu), который создан консорциумом поставщиков подвижной связи и поставщиков услуг интернета в Европе.

Поскольку контент и услуги становятся все богаче, все пользователи будут продолжать пользоваться советами и напоминаниями о природе услуги, которую они используют, и о ее безопасном использовании. Например, многие операторы также выстраивают общие руководящие указания для своих интерактивных услуг (например, чатов), которые напоминают пользователям о соответствующем и безопасном поведении, например, путем напоминания пользователям о том, что не следует сообщать свои контактные данные и так далее (см. параграф "Обучение детей" в разделе, посвященном поставщикам услуг интернета, приведенный выше, для дальнейших примеров). Кроме того, в качестве передового опыта многие операторы будут теперь отправлять регулярные напоминания пользователям услуги, предоставляемой с учетом местоположения пользователя (LBS), которая позволяет определить местоположение пользователя, сообщая им, что услуга действует и напоминая им, как изменить свой профиль или отключить услугу.

[9] http://www.sfr.fr/media/pdf/offre-sfr/maj-240107/att00013578/701.09Guideparents2007.pdf

[10] http://www.vodafone.ie/download?id=ICIA_PARENTS_GUIDE.PDF

Ситуационное исследование: Канал CBBC для обучения компьютерной грамотности в Соединенном Королевстве

На CBBC (BBC для детей) есть раздел обучения компьютерной грамотности в обращению со средствами связи, он называется Stay Safe (будь в безопасности), и ведет его мультипликационный персонаж кролик по имени Dongle. Исследование показало, что дети младшего школьного возраста очень хорошо реагируют на этого персонажа. В раздел включены интерактивная викторина, "популярное видео"и ссылки на другие ресурсы, например, "thinkuknow". Этот материал охватывает безопасность в онлайновой и мобильной среде, и содержание выстроено вокруг умных (SMART) правил Stay Safe:

S = Оставайся в безопасности.

M = Не знакомься.

A = Получение электронных писем может быть опасно.

R = Доверяешь? Люди могут быть не теми, за кого себя выдают.

T = Расскажи взрослым, если тебе страшно или неуютно.

На раздел Stay Safe ссылаются все общедоступные веб-страницы, и эти сообщения подкрепляются хостами, так как они поддерживают правильное поведение пользователей. Но важно отметить, что хотя правила SMART широко используются и известны, в пределах отрасли используется несколько разных их версий, которые могут ввести в заблуждение некоторых детей.

Исследование: Серия рассказов в киберпространстве "Жили-были…", MDA и Okto, Сингапур

Сингапурская организация по развитию средств связи (http://www.mda.gov.sg/) поддержала создание анимационного сериала из шести эпизодов, прошедших в эфире на канале медиакорпорации Okto в течение шести недель, которые были созданы для рекламы преимуществ интернета и новых средств связи, вместе с тем подчеркивая необходимость быть осторожнее в онлайновой среде. Эта инициатива была создана в соответствии с поставленной правительством Сингапура задачей по расширению обучения благополучию и безопасности в кибермире.

Сериал предназначен для детей 10–14 лет, в нем действуют персонажи известных сказок, но в современных условиях, их сюжет связан с новыми средствами связи и интернетом.

Например, в первом эпизоде – "Красная Шапочка, использующая мгновенный обмен сообщениями". Красная Шапочка выходит он-лайн и обнаруживает сообщение от незнакомой девочки, которая живет в другой части леса. Красная Шапочка начинает болтать с девочкой и в конце говорит, что она собирается навестить бабушку и даже говорит ее адрес. Серия продолжается, и мы обнаруживаем, что "девочка" на самом деле – это "маска" Злого Волка.

Сюжет других пяти эпизодов: Белоснежка и онлайновые игры, Пиноккио отправляется на свидание вслепую, Три поросенка и атака вируса из интернета, Спящая Красавица и ее мобильный телефон, а также Большой и Злой Задира из интернета – можно найти на веб-сайте MDA: http://www.mda.gov.sg/wms.file/mobj/mobj.1334.Annex.pdf.

Ситуационное исследование: использование средств связи потребителя для поддержки усилий по борьбе со спамом и мошенническими СМС

Потребители, включая подростков и детей, могут столкнуться с двумя видами возможного мошенничества с применением СМС, на которые, если бы это была правильная информация, можно было бы охотно ответить.

СМС можно использовать для отправки сообщений с просьбой перезвонить или отправить обратное сообщение на номер услуги с премиальной выплатой. Обычно сообщение имеет вид: "Поздравляем! Вы выиграли приз! Позвоните на номер XXX XXX XXX [номер с премиальной выплатой], чтобы получить подробную информацию". Этот вид мошенничества, или "микрожульничество", предназначен для снятия денег с предоплаченного баланса или счета пользователя.

В вариации с фишингом потребители могут получать сообщения на свои подвижные устройства для кражи идентичности мошенническим образом. Например, потребитель может получить текстовое сообщение или голосовую почту якобы от налогового инспектора, в котором говорится, что человеку должны вернуть часть суммы, и когда потребитель перезванивает, они вынуждают его сообщить его данные о банковском счете.

В таких случаях операторы должны проводить обучающие кампании, чтобы помочь пользователям понять и определить, обман таких мошенников, тем самым избегая его, (например, узнать код номеров телефонов с премиальными выплатами и не звонить на номера, начинающиеся с этого кода, отвечая неизвестным абонентам). Где возможно операторы должны сообщать об источниках, где содержатся последние обзоры существующих мошенничеств, см. например, сайт SCAMwatch (http://www.scamwatch.gov.au/), который поддерживается Комиссией Австралии по лотереям и потребителям, и который имеет цель "помочь вам определить, сообщить и защититься от мошенничеств", и имеет раздел, посвященный "мошенничествам при помощи мобильных телефонов ".

Другая основная форма злоупотребления основана на СМС с премиальной выплатой, используемых для предложения услуг с абонентской платой. Услуги с абонентской платой предлагаются на законных основаниях для регулярных транзакций, например, при покупке еженедельно одной и той же информационной услуги. Злоупотреблением СМС-услугами с абонентской платой является случай, когда поставщик информационных услуг заставляет потребителя думать, что услуга оказана один раз или на основе разового платежа, но она оказывается повторно или в рамках услуги с абонентской платой. Примером может быть объявление в журнале, создающее впечатление одноразовой услуги, но на самом деле являющееся услугой с абонентской платой. Пользователи должны отменить последующие платежи за услугу.

Когда пользователи сталкиваются с мошенническими СМС, они должны иметь возможность пожаловаться оператору сети и/или национальному органу, регулирующему услуги связи или премиальных выплат, например, иметь возможность переслать СМС на определенный, известный номер мобильного телефона. Повторяющиеся жалобы помогают отрасли определять нечистоплотных поставщиков и предпринимать соответствующие действия, вплоть до создания условий для нерентабельности таких действий.

Обращая внимание своих пользователей на следующие типы сооб

щений, операторы могут помочь своим пользователям в защите от СМС, содержащих спам и мошенничество:

- Не реагируйте на просьбы позвонить на дорогостоящие номера с премиальной выплатой – люди, отправляющие вам СМС с просьбой перезвонить, используют обычные номера подвижной связи. Даже, если вы не узнали номер вызывающего абонента, вы можете избежать такого мошенничества, определив и запомнив национальные коды номеров с премиальной выплатой в вашей стране (часто они начинаются с 09).
- Организаторы лотерей не отправляют сообщение о выигрыше случайным образом – если вы видите, что это не извещение о выигрыше, скорее всего это мошенничество.
- Если вы приобретаете рингтон или другую услугу и обнаружили, что вам регулярно высылают сообщения, возможно, вы согласились на мошенническую подписку по СМС. Отмените дальнейшие выплаты, сославшись на изначальное объявление, и пожалуйтесь вашему оператору и в соответствующий национальный регуляторный орган.
- Точно так же, если операторы ввели дополнительные механизмы для сообщений о спаме, это должно быть объявлено пользователям. Операторы подвижной связи во Франции, например, поддержали запуск сокращенного кода СМС и специальный веб-сайт для сообщений пользователей о СМС, содержащих спам, http://www.33700-spam-sms.fr/

5. Незаконный контент

Учитывая те же самые приоритеты, операторы подвижной связи из более чем 70 стран и представляющие интересы более 900 млн. потребителей, которые подписали Свод правил по спаму Ассоциации GSM (GSMA) и которые должны делать все для обеспечения того, "чтобы процессы, которые они используют для получения согласия [при приеме рекламного сообщения] были ясными и прозрачными" и предоставления потребителям "понятных, ясных и эффективных средств для отказа от дальнейшего получения от оператора подвижной связи рекламных сообщений через СМС или MMS".

Конечно, связь – это двусторонний процесс, и в настоящее время многие операторы предоставляют потребителям функции для связи с ними, позволяющие заявить о возникновении проблем или обсудить проблемы: будь то заявление об обнаружении некорректного контента или контакта при использовании услуги подвижной связи, кража устройства подвижной связи, получение спама или просьба о применении/отключении родительского контроля, – и для выполнения этих функций используется персонал, прошедший подготовку для эффективного реагирования.

Как будет показано ниже, правильная работа с заявлениями потребителей о потенциальном незаконном контенте является ключевым элементом борьбы с существованием незаконного контента, включая материалы, содержащие сексуальное насилие над детьми, в среде подвижной связи.

Все поставщики услуг интернета (подвижной и фиксированной связи) должны сотрудничать с правоохранительными органами для выполнения возложенных на них законом обязательств, относящихся к незаконному контенту. Тем не менее, многие поставщики услуг интернета используют дополнительные способы содействия в борьбе со злоупотреблениями их услугами для незаконного хостинга и/или распространения незаконного контента, включая материалы, содержащие сексуальное насилие над детьми (детскую порнографию). Общепринятые дополнительные меры включают в себя:

- Условия использования и "Руководство пользователя", однозначно запрещающие незаконную деятельность;
- Процедуры предупреждения и отключения (NTD) или процедуры "Запрещения продолжения противоправных действий";
- Совместную работу и поддержание государственных горячих линий.

Условия использования, "Руководящие указания пользователя"

Поставщики услуг интернета, которые предлагают интерактивные услуги, позволяющие пользователям хранить и обмениваться контентом, например, фотоальбомы, сайты социальных сетей, могут применять условия использования их договоров с потребителями, в которых четко обозначены их позиция относительно использования их услуг или распространения незаконного контента, с тем чтобы подчеркнуть свою приверженность сотрудничеству с правоохранительными органами, оставляя за собой все права, в том числе право удалять незаконный контент и право замораживать учетные записи пользователей.

Многие поставщики услуг интернета повторяют и еще раз подчеркивают содержание их условий использования на более легком для понимания, удобном языке в "руководстве пользователя", где изложены правила поведения, ожидаемые от пользователя их услугами. Такие указания для пользователя обычно доступны при непосредственном использовании соответствующей услуги или в момент создания учетной записи для услуги.

Поставщики услуг могут также активно проводить оценку рекламного контента, размещенного на собственных серверах (либо оригинального фирменного содержания, либо материалов, переданных поставщикам по договорам с третьими лицами) на постоянной основе в целях обеспечения того, чтобы незаконное или потенциально опасное содержимое не было доступно через их сеть.

Процедуры предупреждения и отключения

Будь то добровольная мера или требование законодательства, процедуры предупреждения и отключения (NTD) или "запрещения продолжения противоправных действий" являются основным средством защиты операторов или поставщиков услуг в стремлении сохранить свои услуги свободными от незаконного содержания: как только поставщики предупреждены о том, что начато использование их услуг для приема незаконного содержания, они предпринимают шаги по его удалению.

Для эффективного применения мер NTD необходимо обеспечить ясность законодательства относительно характера содержания, которое является незаконным, и правоохранительные органы (или уполномоченные организации) должны быть готовы подтвердить, что отдельные элементы содержания являются незаконными.

Ситуационное исследование: услуги "Горячая линия для случаев насилия"и подход "Предупреждение и отключение"– Telecom Italia

В соответствии с действующими местными законами и законодательством ЕС по вопросам защиты детей, предупреждению киберпреступности и борьбы против материалов, содержащих сексуальное насилие над детьми (детская порнография), Telecom Italia создала оперативные центры для работы с обращениями, связанными с насилием. Эти центры известны как "Горячая линия для случаев насилия", они специализируются на различных типах потребителей: розничная торговля, бизнес и топ-клиенты). Эти центры являются посредниками между пользователями услуг, главным образом, пользователями интернета и Компанией по управлению злоупотреблениями и неправомерным использованием услуг.

При помощи специальных работ, выполняемых операторами, горячая линия для случаев насилия компании Telecom Italia может управлять различными типами киберпреступлений, сообщая в компетентные местные органы обо всех относящихся к делу фактах или значимых событиях, таких как наличие материалов, содержащих сексуальное насилие над детьми, в сетях Группы или на ее сайтах.

В действие введены два весьма важных способа предотвращения: первый – механизм снятия материалов на основании уведомления (NTD), при котором либо пользователи, либо полиция уведомляют операторов горячей линии для случаев насилия о незаконном контенте сайтов, который должен быть удален; второй способ – система фильтрации на базе веб, используемая во всех сетях Telecom Italia, которая основана на методах фильтрации DNS и IP и способна запрещать доступ к определенным сайтам в домене или к списку различных адресов IP; списки DNS или адресов IP, подлежащих блокированию, предоставляются в Италии общественной организацией CNCPO (Национальный центр по борьбе с детской онлайновой порнографией), и эти списки автоматически загружаются каждый день.

Операторы и поставщики услуг могут взять на вооружение или поддержать Горячую линию в интернете, линии помощи или специализированные веб-сайты в целях управления, сокращения или ликвидации киберпреступности и незаконных материалов на своих веб-сайтах или инфраструктуре. Таким образом, они могут получать сообщения о незаконном контенте от потребителей, представителей общественности, органов охраны правопорядка или организаторов горячей линии (см. ниже). Если сообщение получено от представителя общественности, например, через службу технической поддержки, операторы/поставщики услуг интернета передают информацию органам охраны правопорядка или, при необходимости, на государственную горячую линию, например, чтобы проверить, действительно ли контент является незаконным, или предпринять какие-либо дальнейшие законные меры.

Организаторы горячих линий

К 1995 году, когда популярность интернета стала расти, для отрасли, а также для органов власти и органов охраны правопорядка стало ясным, что интернет начал использоваться для публикации и обмена незаконным содержанием, в частности, материалов, содержащих сексуальное насилие над детьми. Началось обсуждение различных путей решения этой проблемы, включая создание специальной горячей линии для людей, желающих сообщить о незаконном контенте в он-лайне.

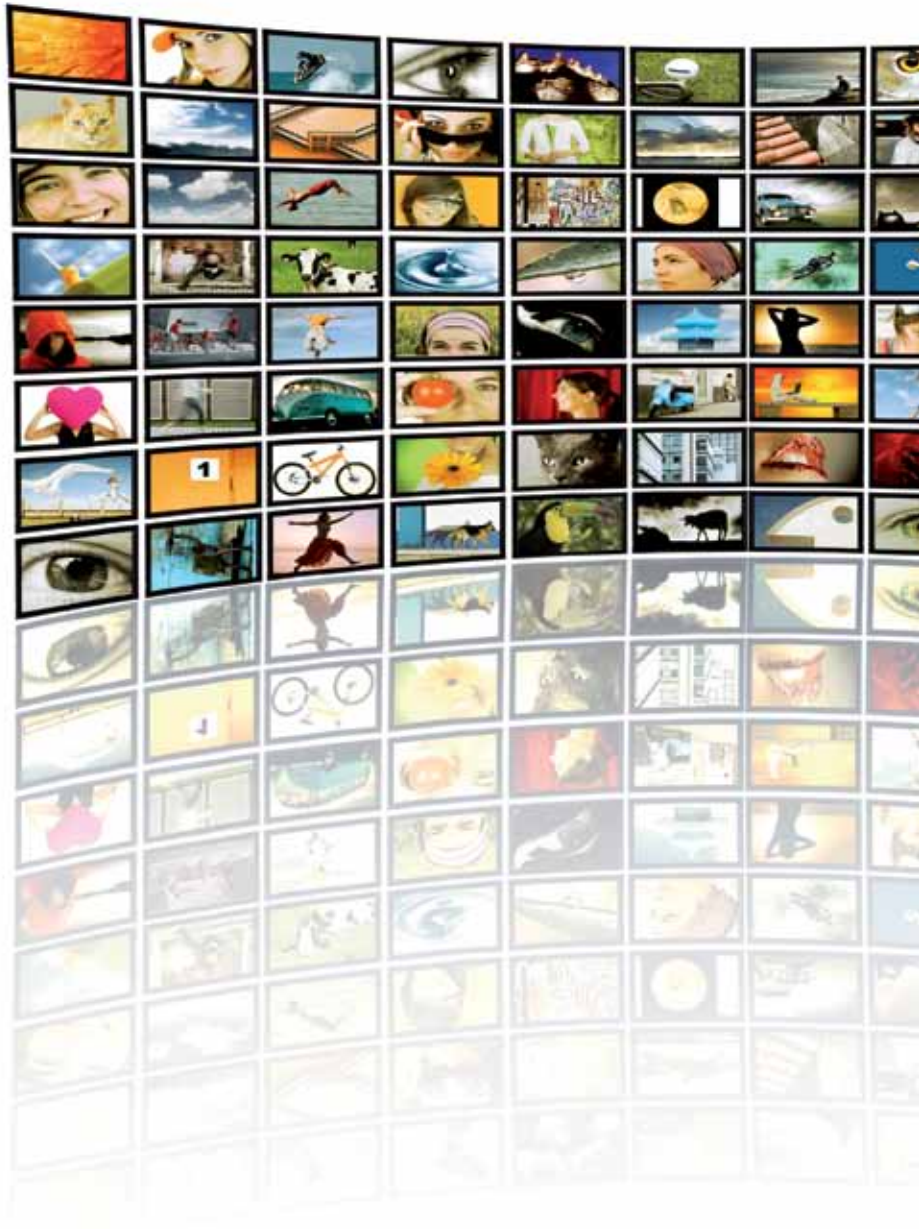
Первая горячая линия для сообщений о материалах, содержащих сексуальное насилие над детьми, была запущена в Нидерландах в июне 1996 года в качестве совместной инициативы отрасли, правительства и органов охраны правопорядка. За этим последовали аналогичные инициативы в Норвегии, Бельгии и Соединенном Королевстве.

С тех пор многие страны создали горячие линии и INHOPE (Международная ассоциация горячих линий интернета) – головная организация для горячих линий насчитывает около 30 полноправных членов, представляющих горячие линии по всему миру.

Помимо стандартных подходов NTD по управлению незаконным контентом, размещенным на их собственных сервисах, операторы, поддерживающие и продвигающие местные горячие линии, обеспечивают потребителям и представителям общественности средства сообщения о незаконном содержании при его обнаружении, и это является важным шагом в деле содействия борьбе с незаконным контентом, включая материалы, содержащих сексуальное насилие над детьми.

Сотрудничество в рамках отрасли

Кроме того, существует ряд совместных отраслевых инициатив, таких как Технологическая коалиция, Финансовая коалиция против детской порнографии и Мобильный альянс против материалов, содержащих сексуальное насилие над детьми. Эти инициативы объединили целый ряд ведущих участников рынка в рамках их отраслей с целью обмена знаниями и развития технических средств и новых способов борьбы с наличием онлайновых материалов, содержащих сексуальное насилие над детьми, от имени более широкого представительства отрасли, в том числе, например, путем блокирования доступа к URL, о которых известно, что они содержат материалы с сексуальным насилием над детьми.



6. Другие вопросы

Контент, созданный пользователем (UGC): подход радиовещательной организации

В этом разделе описываются подходы, которые могут использовать радиовещательные организации в целях борьбы с контентом, создаваемым пользователем с применением их услуг (UGC).

Для того чтобы на форуме не размещался недопустимый контент, рекомендуется, чтобы радиовещательные организации ввели в действие целый ряд процедур по защите онлайновых пользователей от недопустимого созданного пользователем содержания. К ним относятся:

a) Автоматические фильтры – нежелательные слова могут быть блокированы в именах и сообщениях пользователей в момент размещения сообщения. Этот фильтр включает ненормативную лексику, сексуальную лексику, расистские и гомофобские выражения. Также могут быть блокированы чужие URL, наряду с адресами электронной почты.

b) Предварительная модерация – к примеру, все форумы могут предварительно модерироваться специальной командой модераторов контента для детей, следящих за содержанием, которое противоречит опубликованным правилам работы. Каждое сообщение может быть проверено до его опубликования, а модераторы также обнаружат и отметят подозрительных пользователей, а также пользователей, попавших в беду.

c) Хостинг – в дополнение в команде модераторов может существовать команда сообщества хостингов. Сообщество хостингов управляет форумом с общественной точки зрения, и они могут служить отправ-

ной точкой связи с модераторами, когда возникают вопросы о пользователе.

Вся модерация должна выполняться работающей в офисе командой, члены которой прошли тщательные проверки сторонней организацией с целью определения, имели ли они прежде судимости. Кроме того, команда модераторов должна соблюдать следующие правила:

- Запрещается работа на дому, в целях обеспечения того, чтобы никто не имел доступа к информации о детях;
- Модерация должна быть командной с тем, чтобы модераторы в группе могли обсудить озабоченность относительно сообщений или пользователей и наращивать свои знания о поведении пользователей;
- Модерация должна производиться в соответствии с жесткими правилами руководящих указаний по модерации, созданных за время существования ресурса;
- Модераторы должны иметь определенные часы работы и форумы должны быть открыты только в эти часы. Поэтому когда форумы открыты для размещения сообщений, всегда присутствует дежурный модератор.

Тем не менее, это очень трудоемкий процесс, и чем более популярно и успешно сообщество, тем больше ресурсов требуется для его модерации.

Крайней штрафной санкцией является блокирование тех, кто упорно игнорирует опубликованные внутренние правила работы. Однако, в будущем радиовещательные организации могут перейти к системе, в большей мере основанной на принципе "доверие и репутация", поощряющей хорошее поведение, что позволит сверстникам передавать друг другу опыт на собственном примере. Те, кто играет ведущую роль и занимает центральное место в сообществе, будут вознаграждены за хорошее поведение, а нарушители будут удалены. Весь контент, создаваемый и представляемый пользователем, должен быть подвергнут предварительной модерации прежде, чем получит путевку в жизнь.

Особая предварительная модерация общественных чатов, например, любимых детских авторов и ведущих, является стимулом в ее использовании для целевой возрастной группы при участии в онлайновых сообществах радиовещательных организаций. Предложение этих особых мероприятий и другого содержания высшего качества останавливает пользователей от лжи о своем возрасте и регистрации услуг, направленных на взрослых пользователей.

Все чаще радиовещательные организации онлайновых услуг поощряют пользователей отправлять фотографии и видео, а также текст. Все эти материалы должны быть предварительно проверены, с тем чтобы убедиться, что материал пригоден для опубликования на веб-сайтах радиовещательных организаций и что дети не публикуют деликатную личную информацию о себе или других, например, эмблемы школ, названия улиц, номера квартир, которая может подвергнуть их риску, к примеру, посредством "jigsaw id".

В частности, когда видео предназначено для детей, радиовещательные организации должны требовать номер телефона опекуна или родителя, чтобы получить согласие взрослого перед опубликованием. Это соответствует ТВ-правилам и мерам по защите детей, например, от преследования отдельно проживающих родителей, которые по постановлению суда не должны приближаться к ним.

Ситуационное исследование: как радиовещательные организации могут защитить детей от неподобающих, материалов из внешних источников: пример BBC

Все внешнее содержание, на которое есть ссылки на сайтах Cbeebies и CBBC, заранее одобрено экспертом-редактором и помещено в "зеленый"список, в котором позже можно производить поиск силами поисковых служб BBC.

Cbeebies обычно производит поиск содержания на сайте Cbeebies и одобренных под-сайтах, созданных независимыми производителями, поддерживающими их собственную программу Cbeebies.

Инструмент поиска CBBC является более сложным ресурсом, который помогает пользователям найти лучшее содержание как на сайтах CBBC и Newsround, так и на тщательно отобранных сайтах в пределах BBC и более широкого спектра веб-сайтов. Все сайты должны проходить контроль содержания и подходить аудитории Соединенного Королевства в возрасте 7–12 лет и не должны:

- **Содержать, ссылаться или рекламировать порнографические материалы или другие сексуально возбуждающие материалы, если только они являются частью специальной программы по сексуальному воспитанию этой группы аудитории;**
- **Содержать, ссылаться или рекламировать повышенную жестокость или содержание, подстрекающее к жесткому поведению, включая онлайновые игры и обзоры игр с драками, стрельбой или использованием другого оружия;**
- **Подстрекать к чему-нибудь противозаконному;**
- **Подстрекать к дискриминации любого вида;**
- **Рекламировать слабое здоровье/неправильное питание;**
- **Использовать неподобающую лексику;**
- **Существовать только с целью продажи продуктов или услуг;**
- **Поддерживать азартные игры;**
- **Запрещать возможность оплаты абонентам.**

BBC не позволяет ссылаться с сайтов CBBC на сайты любых социальных сетей. Если любой внешний сайт имеет форумы, они должны всегда премодерироваться. На веб-сайтах BBC для детей недопустимо иметь ссылки на чаты.

База данных поиска CBBC постоянно проверяется автоматизированным инструментом, который сканирует все веб-сайты в базе данных, наблюдая за изменениями в соответствии с ключевыми словами, например, "форум"или "чат'.

Если такие изменения обнаружены, сайт будет помечен для исследователя, который снова проверит сайт на пригодность и при необходимости удалит его из базы данных.

Точно так же коммутатор PSB имеет строгие правила, когда приходится защищать пользователей от неподобающего содержания в онлайновой среде. Так как наличие коммутатора на веб-сайтах третьих лиц является важной частью предложений подросткам, позволяющим применение коммутатора людям, которые не очень знакомы с предложениями PSB, все предприятия в этой области полностью модерируются и за ними внимательно наблюдают. BBC включает в коммутатор ссылки на внешние ресурсы в функции безопасности в окружающей среде, когда возможно, и никогда на чаты.

7. Заключение

Для того чтобы ISP и другие поставщики онлайновых услуг могли эффективно работать в рамках Защиты детей в онлайновой среде, важно чтобы они четко понимали, как классифицируются контент и услуги в соответствии с законодательством, под юрисдикцией которого они работают.

Совместная деятельность с местными радиовещательной организациями будет очень полезна в показателях развития такого понимания. Важно также понимать, как местное законодательство классифицирует "местонахождение" содержания и определяет "место", в котором принимается или получается услуга.

Каждая страна несет ответственность за разработку своего законодательства, которое можно применить к контенту и услугам интернета в рамках своей юрисдикции. К сожалению, как показали несколько исследований, во многих стран уровень законодательства недостаточен или не соответствует требованиям, и в итоге не может решать вопросы защиты детей в онлайновой среде.

Кроме того, в разных юрисдикциях наблюдаются разные точки зрения. Эти разные точки зрения могут стать объектом злоупотребления и использоваться в ущерб детям. Преступники и люди, осуществляющие сексуальное насилие над детьми, будут знать, в какой стране самые слабые законы или наименее развитые механизмы борьбы с такими проблемами, и они, конечно же, будут стремиться туда, пока не будут приняты меры противодействия.

Учитывая такую несовместимость законотворческой и политической инфраструктур разных стран, необходимо, чтобы отрасль интернета в целом соответствовала руководящим указаниям по передовому опыту и прини-

мала мировые стандарты и кодексы отраслевой практики, которые позволят им выполнять социально ответственные действия в сфере борьбы с проблемами защиты детей в онлайновой среде.

Во многих странах мира промышленность занимает первое место и утверждает добровольные и саморегулирующие подходы, которые показывают обязательства в отношении создания ответственного подхода к использованию детьми онлайновых ИКТ и связи. Отрасль очень заинтересована в таких действиях, для того чтобы двигаться вперед не только потому, что это правильно с точки зрения морали, но и из-за того, что в дальнейшей перспективе это поможет укрепить общественную уверенность в том, что интернет безопасная среда передачи.

Без этой уверенности и доверия, технология никогда не отдаст нам и не реализует свой огромный потенциал как в обогащении и оказании помощи людям, так и в увеличении экономической состоятельности и благосостоянии каждой страны.

8.

Дополнительная информация и материалы для чтения

Совместная деятельность отрасли

Европейская концепция по безопасному использованию подвижной связи для детей и подростков: http://www.gsmeurope.org/documents/safer_children.pdf

Ссылки на национальные правила работы операторов подвижной связи Европы (на английском и их родном языке): http://www.gsmeurope.org/safer_mobile/national.shtml

GSMA, правила работы со спамом: http://www.gsmworld.com/our-work/public-policy/protecting-consumers/mobile_spam.htm

Программа безопасного интернета: помощь и защита детей в онлайновой среде: http://ec.europa.eu/information_society/activities/sip/index_en.htm

Программы Telecom Italia по защите детей: www.telecomitalia.com, Устойчивость ->горячие темы -> Защита детей и жестокое обращение

Исследование в рамках Программы безопасного интернета по сравнению эффективности программного обеспечения и служб фильтрации:

http://ec.europa.eu/information_society/activities/sip/projects/ targeted/filtering/sip_bench/index_en.htm

Министерство внутренних дел: Оперативная группа в области интернета по защите детей (Соединенное Королевство) – документы с примерами передового опыта в отрасли: http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce

Классификация содержания

Созданная отраслью Независимая организация по классификации подвижного содержания Соединенного Королевства: http://www.imcb.org.uk/

Проект EC Kids Online: http://www.eukidsonline.net/

Безопасность детей в цифровом мире: Отчет Byron Review: http://www.dcsf.gov.uk/byronreview/

Средства связи образования и потребителя

Созданный отраслью ресурс для учителей для помощи в понимании того, как подростки используют технологию: http://www.teachtoday.eu/

Нелегальное содержание

Международная ассоциация горячих линий по вопросам интернета: https://www.inhope.org/

Альянс подвижной связи против содержания с сексуальным насилием над детьми

http://www.gsmworld.com/mobilealliance

Финансовая коалиция против детской порнографии

http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=3703

Саморегулирование среды передачи

Все онлайновые службы BBC подчиняются Руководящим редакторским указаниям BBC (http://www.bbc.co.uk/guidelines/editorialguidelines/edguide)

и Руководящим указаниям для онлайновых служб BBC (http://www.bbc.co.uk/guidelines/editorialguidelines/onguide)

Отчеты на национальном уровне

Соединенное Королевство: Безопасность детей в цифровом мире: Отчет Byron Review, http://www.dcsf.gov.uk/byronreview/

Фотографии представлены: www.shutterstock.com, Violaine Martin/ITU, Ahone Ayeh Njume-Ebong/ITU

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

Отпечатано в Швейцарии
Женева, 2011 г.

При поддержке:

TELECOM ITALIA

AfrISPA
African Internet Service Provider's Association

EBU·UER

GSMA

CHIS

vodafone