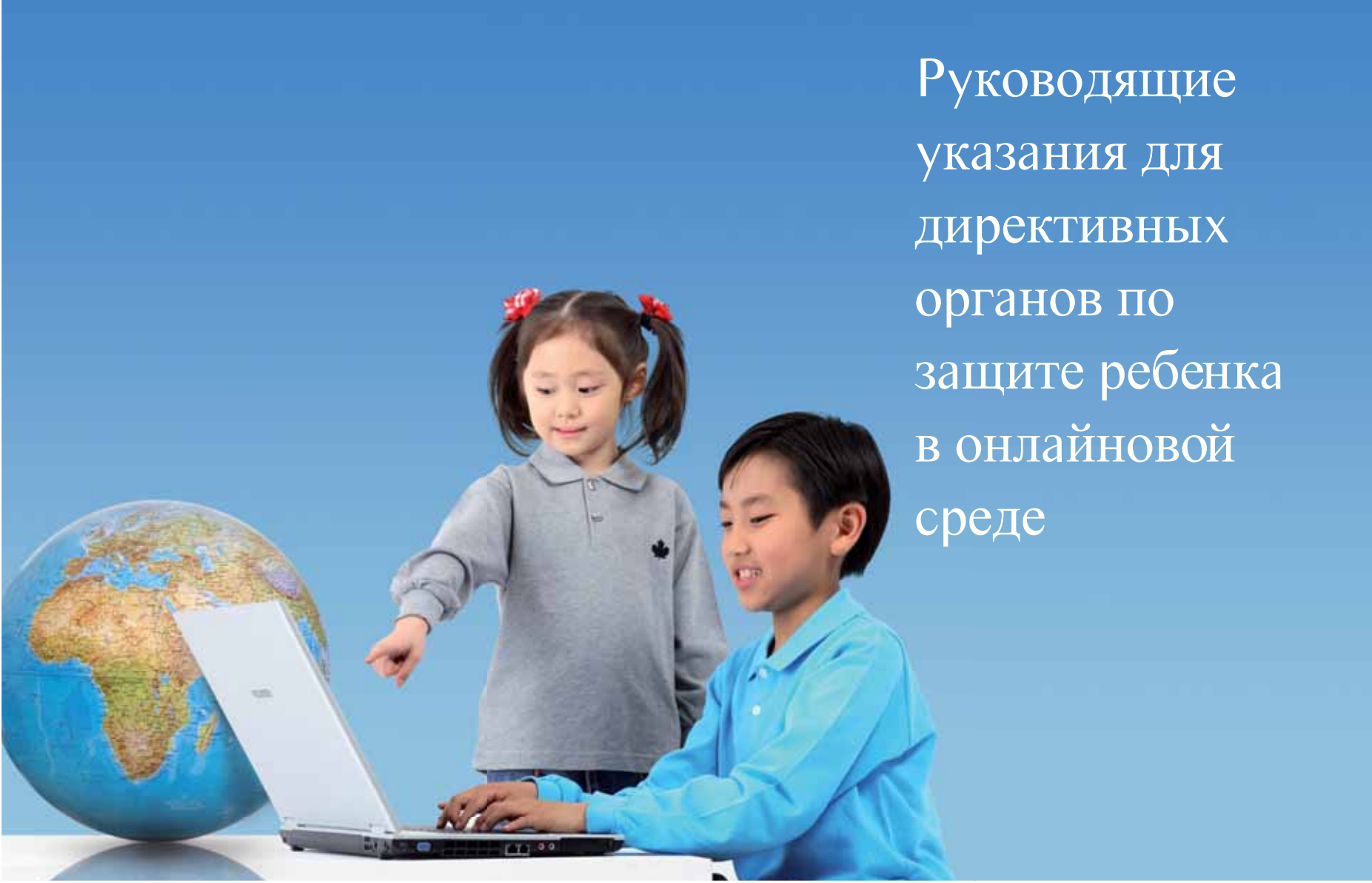


Руководящие указания для директивных органов по защите ребенка в онлайновой среде

www.itu.int/cop

БЛАГОДАРНОСТИ

Данные Руководящие указания подготовлены Международным союзом электросвязи (МСЭ) и командой авторов из ведущих организаций, работающих в отрасли информационно-коммуникационных технологий (ИКТ) и занимающихся проблемами защиты детей. Эти Руководящие указания не смогли бы состояться без затраченного авторами времени, присущего им энтузиазма и самоотверженности.

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

- Кристина Буети (Cristina Bueti) и Сандра Панди (Sandra Pandi) – МСЭ,
- Джонн Карр (John Carr) – Детская благотворительная коалиция за безопасность интернета,
- Рауль Чиезв (Raoul Chiesa) и Франческа Боско (Francesca Bosco) – Межрегиональный научно-исследовательский институт Организации Объединенных Наций по вопросам преступности и правосудия,
- Катерина Каммингс (Catherine Cummings) и Джессика Сарра – Международный центр по пропавшим без вести и эксплуатируемым детям,
- Майкл Моран (Michael Moran) – Интерпол.

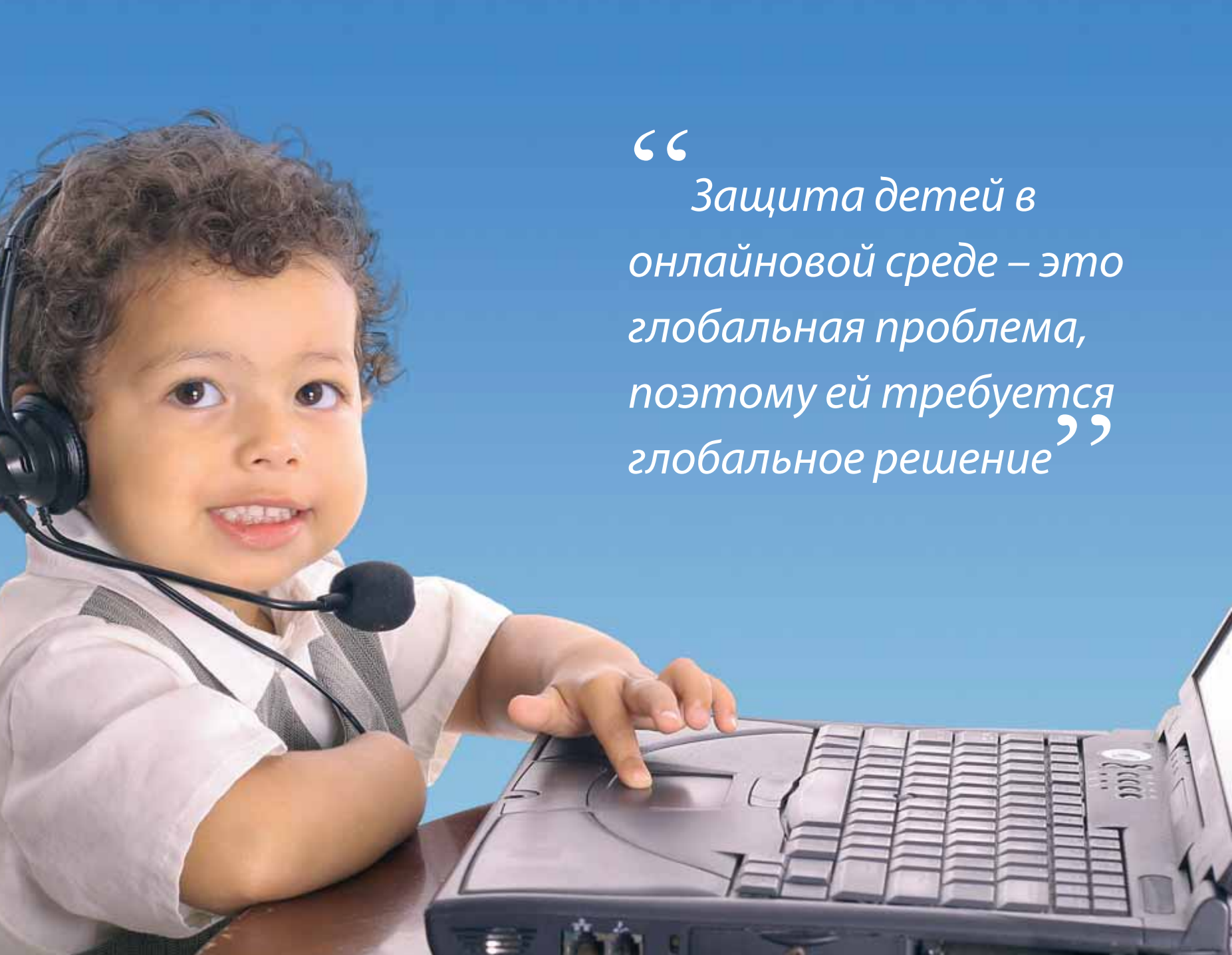
Авторы хотели бы поблагодарить Кристин Квиннь (Kristin Kvigne) из Интерпола за подробный разбор и комментарии.

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 с г-жой Кристиной Буети по адресу: cop@itu.int.

Содержание


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

Предисловие

Я с радостью пользуюсь этой возможностью прочесть вместе с вами предварительный вариант Руководящих указаний, которые разработаны при бесценной 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 международная кооперация могла бы стать ключом к нашему успеху на поле предстоящей битвы

Директивные органы – ключевые участники победы 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

Десять лет назад примерно 182 миллиона человек во всем мире имели доступ в интернет, и почти все они жили в развитом мире. Интересно, что к началу 2009 года во всем мире было более 1,5 миллиарда пользователей интернета, причем более 400 миллионов из них пользуются широкополосным доступом. Сегодня пользователи интернета распространены по всему миру, хотя и не повсеместно, более 600 миллионов пользователей имеется в Азии, 130 миллионов в Латинской Америке и в Карибском бассейне, и 50 миллионов в Африке[1]. Интернет продолжает оставаться динамичным и невероятным ресурсом с почти безграничными возможностями по решению общественных проблем от улучшенного доступа к возможностям здравоохранения до возможностей дистанционного образования и электронного правительства и новейших высокооплачиваемых рабочих мест. Однако растущие глобальные проблемы, окружающие онлайновую кибербезопасность, требуют глобальных решений, особенно когда это касается защиты самых маленьких и наиболее уязвимых цифровых граждан – наших детей.

В соответствии с последними обзорами свыше 60% детей и молодых людей ежедневно разговаривают в чатах. Трое из четырех детей готовы поделиться личной информацией о себе и своей семье в обмен на товары и услуги, и каждый год один из пяти детей мог быть мишенью интернет-хищника.

Эти Руководящие указания подготовлены в рамках инициативы Защита ребенка в онлайновой среде (COP)[2], для того чтобы создать основу безопасного и защищенного кибермира для будущих поколений. Предполагается, что они будут действовать в качестве плана, который может быть адаптирован и использован таким образом, который согласуется с национальными или местными обычаями и законами. Кроме того, их ценность повышается от того, что эти Руководящие указания рассматривают вопросы, которые могут влиять на всех детей и молодых людей, не достигших 18 лет, но каждая возрастная группа будет иметь свои потребности

Данные Руководящие указания подготовлены МСЭ и командой авторов из ведущих организаций, работающих в отрасли ИКТ и занимающихся проблемами онлайновой защиты детей, а именно, Детская благотворитель-

[1] Всемирная база данных показателей ИКТ 2008 г., 12- е издание

[2] www.itu.int/cop

ная коалиция за безопасность интернета (CHIS), Международная линия помощи детям (CHI), Международный центр по пропавшим без вести и эксплуатируемым детям (ICMEC), Интерпол и Межрегиональный научно-исследовательский институт Организации Объединенных Наций по вопросам преступности и правосудия (UNICRI).Неоценимые вклады были также получены от правительств отдельных стран и высокотехнологичных компаний, которые разделяют общие цели – сделать интернет лучшим и более безопасным местом для детей и молодых людей.

Мы надеемся, что это приведет не только к созданию всеохватывающего 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[3], принятой в соответствии с Резолюцией 44/25 Генеральной Ассамблеи ООН от 20 ноября 1989 года и Итогового документа[5] Встречи на высшем уровне по вопросам информационного общества[4] (ВВУИО) .

На ВВУИО лидеры международного сообщества поручили МСЭ выполнение Направления действий С5 Плана действий: "Создание доверия и безопасности при использовании ИКТ". В Итоговом документе ВВУИО также отдельно признаются потребности детей и молодых людей и защита их в киберпространстве. Тунисское Обязательство признает "роль ИКТ в защите детей и в ускорении развития детей", а также потребность в "усилении действий по защите детей от эксплуатации и защите их прав в контексте ИКТ".

Публикуя данные Руководящие указания, Инициатива COP призывает все заинтересованные стороны обеспечивать принятие правил и стратегий, которые будут защищать детей в киберпространстве и способствовать более безопасному доступу ко всем замечательным возможностям, которые могут предоставить онлайновые ресурсы.

[3] www.unicef.org/crc/

[4] ВВУИО проводилась в два этапа: в Женеве 10–12 декабря 2003 года и в Тунисе 16–18 ноября 2005 года. ВВУИО взяла обязательство "построить ориентированное на интересы людей, открытое для всех и направленное на развитие информационное общество, в котором каждый мог бы создавать информацию и знания, иметь к ним доступ, пользоваться и обмениваться ими". См. www.itu.int/wsis.

[5] www.itu.int/wsis

Руководящие указания для директивных органов

Для того чтобы сформулировать национальную стратегию, направленную на безопасность детей в онлайновом режиме, директивные органы должны рассмотреть широкий комплекс мер. Ниже приведено несколько ключевых областей, требующих рассмотрения. Дополнительные предположения можно также найти в Приложении 4.

	№	Ключевые области, требующие рассмотрения
Правовая база	1	Пересмотреть существующую правовую базу, чтобы установить, что имеются все необходимые юридические права, для того чтобы правоохранительные органы и другие организации защищали людей в возрасте моложе 18 лет в онлайновом режиме на всех платформах доступа в интернет.
	2	Установить, *с учетом необходимых изменений*, что любое действие против ребенка, которое является незаконным в реальном мире, является незаконным в онлайновом режиме, и что правила защиты данных и конфиденциальности в онлайновом режиме применимы также и для несовершеннолетних.
Правоох-ранительные ресурсы и механизмы обратной связи	3	Обеспечить создание и широкую известность механизма по предоставлению понятных правил относительно того, как сообщать о незаконном контенте, обнаруженном в интернете, например, государственная горячая линия, которая имеет возможность быстрого реагирования и удаления незаконного материала или запрета доступа к нему.

	№	Ключевые области, требующие рассмотрения
Национальные особенности	4	Свести воедино усилия всех соответствующих сторон, заинтересованных в вопросах безопасности детей в онлайновом режиме, в частности: • Правительственных организаций • Органов охраны правопорядка • Организаций социального обслуживания • Поставщиков услуг интернета (ISP) и поставщиков других электронных услуг (ESP) • Поставщиков услуг подвижной телефонии • Других соответствующих высокотехнологичных компаний • Родительских организаций • Учительских организаций • Детей и молодых людей • НПО по защите детей и других соответствующих НПО • Академических и исследовательских организаций • Владельцев интернет кафе и других поставщиков услуг коллективного доступа, например, библиотеки, центры связи, помещения PC Bang [6] и центры онлайновых игр и т. д.
	5	Рассмотреть возможные преимущества разработки модели саморегулирования или совместного регулирования, выраженной посредством публикации кодексов добросовестной практики, как в свете оказания содействия привлечению и сохранению вовлеченности всех заинтересованных участников, так и в свете повышения скорости, с которой могут быть разработаны и реализованы соответствующие действия в ответ на технологические изменения.
Образовательные ресурсы и повышение осведомленности	6	Использовать знания и опыт всех заинтересованных участников и разработать сообщения и материалы о безопасности в интернете, которые отражают местные культурные нормы и законы, и обеспечить, чтобы они были эффективно распределены и соответствующим образом представлены всем представителям основных целевых аудиторий. Рассмотреть возможность подключения помощи средств массовой информации в распространении сообщений, повышающих осведомленность. Разработать материалы, которые подчеркивают положительные и действенные аспекты интернета для детей и молодых людей и позволяют избегать пугающих сообщений. Пропагандировать положительные и ответственные формы поведения в он-лайне.
	7	Рассмотреть роль, которую могут играть технические средства, например, фильтрующие программы и программы обеспечения безопасности ребенка в качестве поддержки и дополнениям образовательных инициатив и инициатив повышения осведомленности.
	8	Призывать пользователей нести ответственность за свои компьютеры, стимулируя регулярное сервисное обслуживание, предусматривающее обновление операционной системы, установку и обновление брэндмауэра и антивирусных программ.

[6] "PC Bang" – термин, широко используемый в Южной Корее и в некоторых других странах для описания большой комнаты, в которой по локальной сети осуществляется широкомасштабное участие в компьютерной игре, либо в онлайновой, либо между игроками в комнате.

1. Базовая информация

Технология, которую мы сегодня называем "интернетом" зародилась в 1950-х годах и даже ранее. Однако в начале 1990-х только разработка Всемирной паутины (World Wide Web) стала толчком к экспоненциальному росту интернета, что привело к тому, что он стал чрезвычайно ценным аспектом нашей жизни, как в экономическом, так и в социальном плане, и похоже вывела его на позиции основной характерной черты современной жизни.

На самой заре интернет-революции пользователей привлекала возможность общаться с людьми и получать информацию через океаны и временные пояса при помощи нескольких щелчков мышки. Однако для того чтобы это сделать, они, как правило, должны были находиться в стационарном месте перед монитором большого громоздкого компьютера, обычно ПК.

Сегодня люди могут присоединиться к глобальной сети, используя мобильный телефон, лэптоп или другие портативные устройства, которые часто имеют функции работы с видео и очень высокоскоростной доступ. Многие игровые консоли также способны работать с интернетом, и все это лежит в основе стремительного роста увлечения онлайновыми играми среди детей и молодых людей.

Мобильной телефонии потребовалось примерно 20 лет, для того чтобы достичь миллиарда пользователей, тогда как на второй миллиард потребовалось всего несколько лет. В отличие от мобильной связи фиксированной телефонии, для того чтобы набрать свой первый миллиард пользователей, потребовалось 125 лет.

Эволюция от второго до третьего поколения мобильных телефонных сетей вероятно так

“Сведем воедино всех заинтересованных участников процесса обеспечения безопасности детей в онлайновом режиме”

же значительна, как и первый скачок от аналоговой телефонии к цифровой. Она началась более десятилетия назад и идет полным ходом. Недавно появившиеся технологии четвертого поколения продолжают придавать особое значение подвижному доступу, но с еще более высокими скоростями. Конвергенция широкополосных сетей и средств информации создает новые пути для распространения цифровых развлекательных программ.

Устройства пользователей теперь стали многофункциональными и становятся все более персонализированными. В ближайшем будущем успехи в подключении компьютеров к интернету позволят сотням миллионов объектов получить возможность общаться друг с другом по интернету, открывая неисчислимое множество приложений для бизнеса и домашних применений.

Для рынка как фиксированной, так и сотовой связи переход к сетям с более высокой пропускной способностью сопровождается переходом к сетям на основе протокола IP. Следовательно, расширяется использование технологии передачи голоса по протоколу Интернет (VoIP), например при помощи таких услуг как Skype или Vonage, а также расширяется возможность смотреть подвижные изображения по сетям на основе IP. Новые технологии, такие как цифровое телевизионное вещание и цифровое мультимедийное вещание, дадут возможность зрителям просматривать потоковый контент на мобильных устройствах в любое время, в любом месте.

Мир развлечений, по-видимому, входит в совершенно новую эру. В то же время цифровая технология имеет значительное влияние на природу общественных взаимоотношений. Мобильные телефоны уже изменили способ общения людей, организации встреч и работу в многозадачном режиме.

Расширение электронной и цифровой инфраструктур дает многим миллионам людей возможности учиться, публиковать знания и общаться в беспрецедентных масштабах. Дети и молодые люди очень часто являются "первопроходцами" принятия и применения новых возможностей, предоставляемых этими новыми зарождающимися технологиями. Это значительно расширяет возможности многих молодых людей и открывает огромные новые возможности в области образования и личного обучения.

Быстрое снижение реальных цен на достижения информационно-коммуникационных технологий, вместе с огромными изменениями и расширениями существующей инфраструктуры, позволяет многим детям и молодым людям использовать преимущества этой технологии, для того чтобы делать и получать то, что не было известно предыдущим поколениям.

Хотя развитие интернета в разных странах и регионах идет по-разному, доступ в интернет имеется почти повсюду. В развивающихся странах, многие линии соединения с интернетом и телефонными сетями используют беспроводные технологии, а не доступ по фиксированной линии; хранение и передача данных становятся децентрализованными и кажутся неограниченными. "Сетевое общество", появление которого предсказывается уже несколько десятилетий, становится реальностью.

С расширением возможностей доступа интернет становится действительно глобальным, предлагая свои преимущества все большему и большему числу людей, включая детей и молодых людей. Культура и экономика страны определит форму развития интернета и повлияет на риски, которым будут подвержены дети, а также то, как проблемы с этими рисками будут решаться различными заинтересованными сторонами. Для решения этой сложной проблемы невозможно дать простую и единственную рекомендацию.

2. Использование интернета детьми и молодыми людьми

Интернет существует уже несколько десятилетий, однако, его природа значительно изменилась с момента его создания. В самом начале он был, главным образом, инструментом для обмена информацией и данными между правительственными организациями и академическими институтами.
В 1980-х годах интернет открыли для широкой общественности.
С появлением Всемирной паутины (World Wide Web) в 1990-х годах, интернет начал развиваться с необычайной скоростью.
В последние годы произошла еще одна революция: возникновение Web 2.0. Технология веб становится более интерактивной, и гораздо больший срез общества обозначает свое присутствие в интернете. Все больше людей присоединяются к сети сегодня, причем очень часто первыми это делают дети и молодые люди.

Хотя развитие веб-технологии открыло интернет для широкой общественности, в течение некоторого времени он напоминал сеть, которой владели и которую населяли, главным образом, правительственные организации, академические институты и коммерческие корпорации. Отдельные лица, как правило, выходят в сеть для получения доступа к информации, которую предоставляли им эти крупные участники. Этот ранний период веб-технологии отмечался следующими характеристиками:

- низкие уровни числа возможных соединений;
- как правило, низкая про-


form
little
term
example
traditional
crafts
store
government
capabilities
public's
wide
using
world
ipv6
interoperable
servers
corporation
global
lagging
influence
may
graphics
generally
interactive
systems
local
infrastructure
databases
blogs
cost
find
standardized
connection
physical
data
access
series
brand
discussions
interconnection
groups
content
communications
terms
synonymous
strict
widely
management
implementations
files
lan
applied
food
communities
encyclopedias
growth
maintaining
areas
standardization
controlling
progressed
logs

пускная способность;
- малые объемы для хранения данных;
- односторонняя связь и доступ.

С течением времени интернет продолжал развиваться, причем особенно важными были четыре аспекта этого развития:

- увеличение доступной по цене пропускной способности;
- увеличение относительно недорогих объемов памяти;
- снижение цены доступа;
- развитие мобильного интернета.

Эти аспекты развития помогли создать новый тип интернета; вместо простого соединения людей с компаниями, организациями и правительствами интернет дал возможность людям связываться друг с другом и стать онлайновыми издателями с собственными правами. Этот новый интернет, который часто называют Web 2.0, имеет следующие характеристики:

- высокие уровни возможности соединений;
- большие пропускные способности;
- высокие уровни емкости памяти;
- персонализированный и интерактивный контакт (контент, создаваемый пользователями).

Разработаны новые инструменты, которые предоставляют пользователям различные средства для общения и для связи друг с другом. Эти инструменты включают в себя: обмен мгновенными сообщениями, чаты и форумы, услуги хостинга для фото и видео материалов и программы децентрализованного обмена файлами (P2P). Взятые вместе, эти и другие технологии, дали толчок феноменальному росту сайтов социальных сетей, которые за небольшой отрезок времен приобрели огромную популярность среди детей и молодых людей.

Интерактивность и контент, создаваемый пользователями

Дети и молодые люди, также как и взрослые проживают все большую часть своей жизни при помощи новых технологий, и в результате природа рисков, которым он подвергаются, неразрывно переплетается с другими аспектами их поведения. В настоящее время уже невозможно провести точную линию между так называемыми "проблемами интернета" и проблемами "реального мира".

Сайты социальных сетей

Качественно новым и очень умным измерением, которое является фирменной маркой сайтов общения в социальных сетях – это способ, при помощи которого они объединили в одном месте несколько существовавших ранее интернет-технологий,

добавили к ним новые возможности и создали очень дружественные интерфейсы. Эти новые интерфейсы сделаны так, чтобы использование различных функций стало абсолютно простым. Все это вместе дало толчок быстрому росту популярности сайтов общения в социальных сетях, которые захватили врасплох множество людей, в основном родителей.

Сайты общения в социальных сетях позволяют пользователям создавать онлайновый профиль, в котором они могут разместить широкий спектр своей личной информации, например, возраст, пол, родной город и интересы. В частности, новые интерфейсы, разработанные сайтами общения в социальных сетях, упрощают процесс персонализации веб-страниц отдельных пользователей, например, добавляя любимую музыку, фотографии и видеоролики. Дети и молодые люди очень творчески подходят к этому процессу. Профили пользователей на сайте общения в социальной сети становятся продолжениями пользователей и важным для них способом рассказать о себе своим друзьям и всему миру.

Самое важное это то, что сайты общения в социальных сетях дают пользователям возможность находить друзей, с которыми они могут обмениваться сообщениями. Аудитория, которая может видеть чей-либо профиль, как правило, зависит от того, как человек использовал настройки секретности сайта. Очень часто, особенно в начале общения в социальных сетях, выяснялось, что дети и молодые люди совершенно не знали о том, что если они не предпримут специальных шагов для ограничения доступа, например, установив свой профиль "секретным" или "только для друзей", то их профили будут полностью открыты для просмотра всем и каждому. Это делало их уязвимыми для интернет-хищников, которые могли указывать ложные данные о возрасте с целью построения взаимоотношений с ребенком или молодым человеком. Были сообщения о случаях, когда некоторые дети и молодые люди передавали свои сексуальные изображения или обменивались ими при помощи мобильных телефонов, это явление известно под названием "секстинг"[7], часто не понимая, что это их изображение может быть как тлетворным для них, так и незаконным, и кроме того, может просматриваться множеством людей, которые могут зайти на сайт или в профиль. В общем сайты общения в социальных сетях выявили проблему, связанную с тем, как управлять контентом, создаваемым пользователями, который является одной из функций, присущих Web 2.0. Некоторые сайты разработали правила модерации, в соответствии с которыми они отыскивают непригодные или незаконные видеоролики или изображения, тогда как другие сайты просматривают только отдельные изображения или видеоролики, если на них обращается внимание в сообщении от того, кто считает их предосудительными и хотел бы их удалить.

Популярность отдельных сайтов общения в социальных сетях часто обусловлена языковыми или религиозными факторами. Вот несколько примеров: MySpace (особенно популярен в Северной Америке), Facebook (наиболее популярен в Северной Америке, Европе и Океании), Hi5 (наиболее популярен в Латинской Америке), Orkut (Латинская Америка), SkyBlog (Франкофонные страны), Live Journal (Россия и СНГ), Friendster (Азиатско-Тихоокеанский регион), Cyworld (Республика Корея и Народная Республика Китай), Linke-dIn (Европа, США и Индия), Last.fm (Северные и Британские страны и Центральная Европа).

[7] Секстинг – относительно новое явление, когда дети и молодые люди подвергают себя риску, размещая на онлайновых ресурсах свои сексуально провокационные изображения, или передавая их друзьям с использованием технологий подвижной связи.

Источник: Проект Руководящих указаний для родителей, опекунов и учителей по защите ребенка в онлайновой среде, МСЭ, 2009 год.

В соответствии с данными компании Danah Boyd[8] онлайновые выражения, персональные профили или другие типы размещаемого контента имею четыре основные характеристики, которые обуславливают дополнительные риски для детей и молодых людей:

1 Продолжающееся существование: Сообщения в сети записываются, и это продлевает срок жизни любого сообщения.

2 Возможность поиска: Поскольку сообщения в сети записываются и идентичность определяется по тексту, инструменты поиска и обнаружения помогают людям найти других людей.

3 Воспроизводимость: Сообщения в сети могут быть скопированы из одного места и помещены в другое так, что нет никакой возможности отличить "оригинал" от "копии".

4 Невидимая аудитория: Практически невозможно узнать, кто может зайти в профиль или в другие средства онлайнового общения. Эта ситуация еще более усложняется тремя вышеупомянутыми характеристиками, поскольку профили могут просматриваться и доступ к ним может быть получен в разное время и из разных мест, отличных от места и времени его первоначального создания.

Обмен мгновенными сообщениями и чаты

Инструменты для обмена мгновенными сообщениями (IM) позволяют людям связываться с другими людьми непосредственно в онлайновом режиме и вести разговор при помощи письменных сообщений и все чаще посредством видеоконференций. Люди могут добавлять имена тех, с кем они знакомы, в свой список контактов и видеть, доступны ли они для разговора, т. е. находятся ли в он-лайне или нет. Эти разговоры или "чаты" могут вестись с одним человеком (двусторонние) или с группой людей (многосторонние). В большинстве программ контент разговора можно сохранить, если это желательно или необходимо. Хорошо известные программы обмена мгновенными сообщениями и чатов включают в себя MSN Chats, Yahoo! Messenger, Google Talk и AOL Instant Messenger.

Программы однорангового обмена файлами

Программы однорангового обмена файлами, которые также называются программами P2P, дают пользователям возможность загружать и скачивать файлы непосредственно на свои устройства хранения данных и с них. Любой, кто использует такую же программу, может отыскать файлы и загрузить их у других людей, которые имеют такие файлы в доступе. Эти программы упрощают обмен знаниями и информацией, но также ведут к нарушению авторских прав и распространению вредоносных программ (malware), например, вирусов и Троянов[9]. Эти сети также используются для распространения CAM. Хорошо известные программы P2P включают в себя Bittorrent, E-mule, E-donkey и Kazaa.

---

[8] Danah Boyd, Fellow at Harvard Law School's Berkman Center forInternet and Society.

[9] Троянский конь, называемый также Трояном, в контексте компьютеров и программного обеспечения описывает класс компьютерных угроз (malware), которые, как кажется, выполняют нужные функции, но на самом деле выполняют неявные вредоносные функции, которые разрешают несанкционированный доступ к компьютеру, на котором они установлены, позволяя сохранить на компьютере пользователям свои файлы или даже видеть экран пользователя и управлять компьютером. См. http://en.wikipedia.org/wiki/Trojan_horse_(computing)

3. Материалы о жестоком обращении с детьми

Определение

Во многих странах фотографии или видеоролики, на которых изображены сцены сексуальной эксплуатации детей и жестокого обращения с детьми, называют либо "детской порнографией", либо "непристойными изображениями детей". Сегодня многие практикующие врачи предпочитают использовать термин "материалы о жестоком обращении с детьми" или CAM, поскольку это название, как кажется, точнее передает реальную природу содержания термина. Именно этот термин, как правило, будет использован в данном документе.

Интернет полностью изменил масштабы и природу производства и распространения CAM.

Сексуальная революция середины 60-х годов, характеризующаяся открытостью выражения и разнообразия сексуальности, возвестила расцвет спроса на порнографию, и магазины книг для взрослых появились во многих европейских и американских городах[10]. Эти магазины и, помимо них, бизнес почтовых рассылок собирал и поставлял огромные объемы порнографии всякого вида и полного спектра жесткости. Спрос на порнографию удовлетворялся множеством ключевых участников рынка по всему миру. Как и всякий вакуум, эта ниша была быстро заполнена предпринимателями, и очень быстро выросла крупная сеть поставок.

Среди порнографии, которая покупалась, продавалась и обме-

[10] O'Donnell and Milner, (2007), Child Pornography, Crime computers and society, Willan.

нивалась, были и фотографии с изображениями сцен сексуальной эксплуатации детей. Законы против материалов о жестоком обращении с детьми (Anti-CAM), принятые в 1977 году в США, в скором времени распространились в Европе, и производство материалов CAM быстро исчезло и ушло в подполье. К 1986 году практически все традиционные пути получения материалов такого рода были полностью перекрыты, повысив возможность полного подавления коммерции в сфере CAM[11].

Исторически трудности обнаружения материалов CAM в то время означали: люди, желающие просматривать материалы CAM, должны были подвергать себя огромному риску и тратить большие деньги, чтобы получить доступ к такому материалу. Все это изменилось с изобретением интернета. Д-р Элвин Купер (Alvin Cooper) говорил о двигателе "тройного А" для киберсексуальности, который легко трансформировать в соответствии с тем, как интернет революционно изменил производство и распространении материалов CAM:

- доступность (Accessibility) – интернет делает материалы CAM доступными 24 часа в сутки, 7 дней в неделю, круглый год;
- доступность по цене (Affordability) – большинство материалов CAM бесплатны и доступны для обмена или простого скачивания; и
- анонимность (Anonymity) – люди искренне верят, что их общение в интернете секретно и скрыто.

Это стимулировало их находить и иметь дело с материалами CAM, поскольку им казалось, что это совершенно безнаказанно. Тот факт, что они бесплатны и доступны, также способствует укреплению их веры в то, что это они безвредны.

В 1997 году Сэр Вильям Уттинг (William Utting) – известный эксперт в сфере детских социальных служб назвал материалы CAM "кустарной промышленностью"[12]. Вероятно, это был последний момент в истории, когда можно было сделать такое заявление. Сегодня это глобальная индустрия. Кажется, ни одна страна от них не защищена.

Очень трудно определить точные размеры или форму того, что на самом деле является подпольным и незаконным бизнесом. Всевозможные оценки были сделаны в разное время относительно числа соответствующих веб-сайтов[13], числа детей, которых заставили сделать свои фотографии[14], и суммарных финансовых объемов рынка этих изображений. Каждый, кто знает, о чем идет речь, не имеет ни малейшего сомнения в том, что в просмотр и распространение материалов CAM вовлечено огромное число людей и что имеются доказательства участия организованной преступности[15] в коммерческом распространении этих материалов. Точно также, не может быть сомнений в том, что количество незаконных изображений, которые сегодня циркулируют в интернете, достигает многих миллионов, тогда как число отдельных детей, изображенных на этих фотографиях, достигает десятков тысяч[16]. И это только те, о ком мы знаем на сегодняшний момент.

Первоначально, один из основных способов распространения материалов CAM через интернет был

[11] Jenkins, P, Beyond Tolerance, 2001, New York University Press.

[12] UK, HMSO, 1997

[13] В своем годовом отчете за 2007 год IWF утверждает, что немногим менее 3000 англоязычных веб-сайтов ответственны за огромное количество изображений жестокого обращения с детьми, которые доступны в он-лайне. Тремя годами ранее американский Исследовательский центр Computer Crime Research Center заявил, что это число превышает 100 000.

[14] По сообщению Интерпола. А также смотрите отчет компании Telefono Arcobaleno. http://www.telefonoarcobaleno.org/pdf/tredicmoreport_ta.pdf

[15] Подробности дела "Reg Pay" на сайте: http://www.usdoj.gov/criminal/ceos/Press%20Releases/ICE%20Regpay% 20PR_080906.pdf

[16] По сообщению Интерпола, упомянутая выше компания Telefono Arcobaleno в своем отчете говорит от 36 000 детей, среди которых" 42% младше 7 лет и 77% в возрасте до 12 лет". http://www.telefono-arcobaleno.org/pdf/tredicmoreport_ta.pdf

основан на использовании новостных групп сети Usenet. Он и до сих пор остается значительным источником, но сегодня используется также и несколько других интернет-технологий. Наиболее важной из них, возможно, является World Wide Web, так как она наиболее доступна и ее проще всего использовать. Однако поскольку в некоторых странах создали большие трудности по использованию веб-технологий для распространения материалов САМ, все чаще и чаще используются другие интернет-технологии. Среди них наиболее значимыми, возможно, являются программы P2P или обмена файлами. Согласно данным Интерпола контролировать программы Peer2Peer технически просто, но общее число людей, вовлеченных в процесс, на практике делают этот контроль очень сложным.

Каждый раз, когда изображение жестокого обращения с ребенком появляется в интернете или скачивается, за этим скрывается очень серьезный подтекст, а именно, что с ребенком повторно обращаются жестоко. Жертвам всю оставшуюся жизнь приходится жить рядом с этими долгоживущими и распространяемыми изображениями. Наилучшим доказательством этого является реакция жертв и их семей, когда они узнают, что эти изображения распространяются или загружены в интернет[17].

По этой причине имеется всеобщее соглашение о том, что как только обнаружено изображение жестокого обращения с ребенком или веб-сайт с такими материалами, очень важно действовать как можно быстрее, для того чтобы удалить изображение, или закрыть веб-сайт, или сделать его недоступным. Для того чтобы упростить этот процесс, разработана система государственных горячих линий. В настоящее время горячие линии действуют более чем в 30 различных странах, и их число растет[18]. Большой рост числа горячих линий крайне необходим как часть возобновленной глобальной компании по прекращению онлайнового трафика материалов САМ.

Еще одной причиной быстрого реагирования с целью удаления веб-сайта или закрытия доступа к любым найденным в интернете незаконным изображениям, является тот факт, что чем дольше они остаются в сети, тем выше вероятность, что кто-то еще найдет их и возможно скачает. Имеются доказательства, позволяющие предположить, что люди, участвующие в скачивании и сборе материалов САМ, наиболее вероятно могут стать участниками контакта с целью совершения преступления или жестокого обращения с детьми в реальном мире. *Из отчета Fantasy to Reality: The Link Between Viewing Child Pornography and Molesting Children. Kim, C (2004).*

В органах охраны правопорядка сделан ряд шагов по улучшению процесса идентификации жертвы на основании материалов, размещенных в интернете. На национальном уровне разработаны и внедрены процессы и системы, что означает, что материалы САМ, изъятые во время следствия или попавшие в руки следователей иным другим путем, изучаются с целью идентификации жертвы жестокого обращения и, следовательно, интернет-хищника.Материалы, которые раньше не рассматривались и которые невозможно отметить, как локально созданные, передаются в международную сеть следователей и национальным специалистам по материалам САМ. Эта сеть развивается на основе Международной базы данных Интерпола по сексуальной эксплуатации детей (ICSE) и координируется секцией Интерпола по торговле людьми вместе с группой специалистов Интерпола по преступлениям против детей.

Задачей этой базы данных является сбор в одном месте всех существующих в интернете материалов САМ, которые попадают в руки органов охраны правопорядка. Эти материалы изучаются сетью специализированных отделений во всем мире, и, там,

[17] Child Molesters: a behavioral Analysis, Kenneth V. Lanning, 2001.

[18] See www.inhope.org

где возможно, направляются в страну происхождения, для того чтобы определить идентичность ребенка, который стал жертвой. Там, где это невозможно, материал вводится в базу данных с указанием подробностей о том, где он был обнаружен, когда и кем.

Мощные поисковые инструменты показывают, просматривались ли эти изображения ранее или нет, поскольку часто изображения, найденные в одной стране, могут содержать ключи, которые помогут установить факт жестокого обращения в другой стране. Иногда на изображении можно увидеть лицо преступника и установить его личность.

ИНТЕРПОЛ и инициатива COP поощряет передовой опыт в этой области, стимулируя создание централизованного национального ресурса, который мог бы управлять всеми материалами, собранными в пределах границ данной страны, создание национального набора хешей и участие в международной деятельности, выполняемой в данной области.

Все это уменьшает трудозатраты следователей, исключает дублирование усилий по всему миру и, в конце концов, приводит к идентификации жертв и установлению преступников.

Гармонизация законов

Принятие всеми странами соответствующего законодательства против злонамеренного использования информационно-коммуникационных технологий (ИКТ) в преступных или иных целях является центральной задачей для обеспечения кибербезопасности. Поскольку угрозы могут возникать в любой точке мира, проблемы по своему масштабу являются международными и требуют международного сотрудничества, содействия в расследовании общих оперативных и процессуальных положений. Следовательно, важно чтобы страны гармонизировали свое законодательство по борьбе с киберпреступностью, защите детей и упрощению международного сотрудничества.

Разработка надлежащего национального законодательства, законодательства по борьбе с киберпреступностью и в рамках этого подхода гармонизация на международном уровне является главным шагом к успеху любой национальной стратегии по защите ребенка в онлайновой среде. В самую первую очередь для этого требуются оперативные законодательные положения, определяющие как преступление такие действия, как компьютерное мошенничество, незаконный доступ, искажение данных, нарушение авторских прав и CAM. Тот факт, что в уголовном кодексе существуют положения, применимые к аналогичным деяниям, совершаемым в реальном мире, не означает, что они могут быть также применены и к деяниям, совершенным в интернете. Следовательно, для определения возможных пробелов важно провести тщательный анализ существующих национальных законов. Следующий шаг – идентифицировать и определить законодательный язык и справочный материал, который может помочь странам в создании гармонизированных законов против киберпреступности и процессуальных правил. Такие практичные инструменты могут быть использованы странами в разработке законодательства против киберпреступности и связанных с ним законов. МСЭ работает в этом направлении с Государствами – Членами Союза и соответствующими заинтересованными сторонами и вносит значительный вклад в достижение глобальной гармонизации законов против киберпреступности.

Международный центр по пропавшим без вести и эксплуатируемым детям (ICMEC) в апреле 2006 года выпустил отчет "Детская порнография: Модельное законодательство и Глобальный обзор". Главной целью этого отчета, который издан уж в пятой редакции, было повышение понимания относительно существующего законодательства по CAM и констатация важности этой проблемы в национальных

политических программах. Исследование затрагивает множество ключевых областей: специальное законодательство по CAM; законы, дающие определение материалам CAM; законы, которые вносят в разряд противозаконных владение материалами CAM, независимо от наличия намерения их распространять; законы, которые касаются компьютерных преступлений, связанных с CAM; и отчетность со стороны поставщиков услуг интернета (ISP).

Документ, содержащий подробные результаты, полученные ICMEC, содержится в Приложении 4. Из отчета видно, что существуют значительные и очень заметные различия в законодательных подходах, принятых в различных странах. Международное сообщество должно найти способ достичь большей согласованности для борьбы с этой глобальной проблемой.

Еще одной целью отчета ICMEC по Модельному законодательству является предоставление рекомендаций относительно областей, в которых требуется законодательство, направленное на различные аспекты материалов CAM и связанных с ними преступлений на всемирной основе. Как и с другими типами киберпреступности владение, производство и распространение материалов CAM часто осуществляется вне зависимости от государственных границ и, следовательно, требует, чтобы законы во всех странах были сравнимыми или юридически эквивалентными, – это и называется гармонизацией.

Преступники, которые сексуально эксплуатируют детей, будь то с использованием компьютеров и интернета, или отправляясь в другие страны, будут предпочитать избирать своими жертвами детей в странах, где отсутствует законодательство или строгие меры наказания, а также в странах, которые не входят в рамки международного сотрудничества. Соответствие международным юридическим стандартам и принятие соответствующих национальных законов и правил является требованием, для того чтобы решать проблемы эксплуатации детей на международном уровне.

Многие страны широко решают проблему эксплуатации детей, когда она относится к труду или другим преступлениям, или они могут запрещать порнографию вообще; однако этих законов недостаточно, поскольку они не рассматривают криминальные аспекты различных форм изображений сексуальной эксплуатации детей и жестокого обращения с детьми. Для того чтобы законодательство было действительно эффективным, страны следует поощрять к принятию специального законодательства, вносящего материалы CAM в разряд противозаконных и охватывающее преступления, являющиеся специфическими для использования технологии и интернета в связи с CAM; в ином случае преступники воспользуются пробелами в законодательстве.

В законе должны быть положения по консолидации ресурсов, для того чтобы выполнять эти специальные законы и для обучения работников юридических органов, органов прокуратуры и органов охраны правопорядка, которым обязательно потребуется успевать за использованием технологии преступниками.

Основные области, вызывающие озабоченность и требующие указаний по принятию законодательства включают следующее:

- дать точное и ясное определение "ребенка" в соответствии с Конвенцией ООН по правам ребенка;
- дать определение "материалов жестокого обращения с детьми" (CAM), которое должно включать в себя соответствующую терминологию из области компьютеров и интернета;
- предусмотреть уголовные преступления, относящиеся к: владению, производству и распространению материалов CAM, включая псевдоизображения, осознанное скачивание или просматривание таких изображений в интернете;
- предусмотреть уголовные наказания для родителей или опекунов, которые со-

глашаются или содействуют участию их ребенка в CAM;
- предусмотреть наказания для тех, кто сообщает другим, где найти материалы CAM;
- дать определение, что попытки совершения преступлений, связанных с CAM, являются уголовным преступлением;
- решить вопросы об уголовной ответственности детей, вовлеченных в CAM. Уголовная ответственность должна относиться к взрослому преступнику, а не жертве – ребенку;
- ужесточить наказания за повторные преступления, для членов организованных групп и других отягчающих обстоятельств, которые должны учитываться при вынесении приговора.

Основное определение материалов CAM должно включать в себя визуальное представление или описание ребенка, вовлеченного в реальные или симулированные действия по демонстрации или выполнению сексуальных действий, или аналогичные псевдоизображения; оно должно также учитывать, каким образом технологии, например, компьютеры, интернет, сотовые телефоны, PDA, игровые консоли, видеокамеры и DVD, используются для упрощения CAM, поясняя, что CAM и все, что связано с ними, является незаконным, вне зависимости от платформы.

Обучение компьютерной криминалистике для органов охраны правопорядка

Помимо оперативных законодательных положений, органы охраны правопорядка нуждаются в необходимых решениях и инструментах для расследования киберпреступности. Такие расследования сами по себе содержат множество задач. Преступники могут действовать практически из любого места мира и принимать меры, для того чтобы скрыть свою идентичность. Решения и инструмент, необходимые для расследования киберпреступности, могут значительно отличаться от тех, что используются в расследовании обычных преступлений.

Интернет, компьютеры, сотовые телефоны, PDA и цифровые устройства всех типов стали незаменимыми инструментами интернет-хищников, стремящихся к сексуальной эксплуатации детей. Технология, при помощи которой эти устройства работают, становится все сложнее и меняется с большой скоростью. Для того чтобы собрать и сохранить важные доказательства, которые оставили преступники, важно чтобы руководители органов охраны правопорядка были бы обучены и обладали техническими знаниями, соответствующими судебным требованиям национальных и международных судов. Следовательно, органам охраны правопорядка, сотрудникам юридических организаций и органов прокуратуры требуется обучение, которое поможет им понимать, как проводить криминалистический анализ компьютерных жестких дисков и других устройств. Это обучение должно проводиться постоянно, для того чтобы держать их в курсе быстрой смены технологий и дать им опыт практической работы.

Существует множество программных пакетов, которые предоставляют инструменты по проведению исследований прочитанных носителей, и в стоимость покупки пакета программ обычно включено и обучение. К несчастью, эти решения зачастую достаточно дороги и не доступны для развивающихся стран. При достаточном финансировании обучение может осуществляться в самих органах охраны правопорядка и частных предприятиях безопасности.

Многие компании частного сектора обладают технологией и знаниями, для того чтобы помочь в проведении такой работы, поэтому для обеспечения надежной помощи по обучению и технической поддержке может

использоваться партнерство государственного и частного секторов.

Международное сотрудничество и обмен данными

Очень важно достичь высокого уровня международного сотрудничества и обмена данными.

Фундаментальная роль МСЭ в соответствии с ВВУИО состоит в том, чтобы создать доверие и безопасность при использовании ИКТ. Главы государств и правительств и другие мировые лидеры, участвующие в ВВУИО, а также Государства – Члены МСЭ поручили МСЭ предпринять конкретные шаги в направлении ограничения угроз и опасностей, связанных с информационным обществом.

ВВУИО посчитала, что Направление действий С5 охватывает широкий спектр тем и заинтересованных сторон. Как подчеркивается в параграфе 110 Тунисского Плана действий, *"Координация деятельности по выполнению решений с участием многих заинтересованных сторон поможет избежать дублирования в работе. Такая координация должна включать, среди прочего, обмен информацией, накопление знаний, обмен примерами передового опыта и помощь в развитии партнерских отношений между государственным/частным секторами и многими заинтересованными сторонами"*.

ИНТЕРПОЛ[19], используя свою сеть, включающую 187 стран, специализируется на упрощении обмена информацией между органами полиции. Эта сеть позволяет осуществить мгновенный обмен информацией между странами и ее передачу при помощи дополнительной системы i24/7 непосредственно в специализированные отделы.

Там, где обмен информацией и следственными материалами входит в юридическую сферу, взаимное сотрудничество по международному расследованию преступлений выполняется в рамках правовой базы и положений двусторонних договоров о юридической взаимопомощи или многосторонних конвенций. Это не всегда пригодно для быстроменяющегося мира интернета.

Несмотря на наличие соглашений, если в стране, где требуется сотрудничество, не существует соответствующих законов, помощь может не быть предоставлена вовсе, либо может быть предоставлена в очень ограниченных объемах. Сторона, предоставляющая информацию, может оговаривать условия ее использования и может требовать конфиденциальности.

Основой является совместный подход, направленный на достижение консенсуса на глобальном уровне по тем общим элементам, которые должны стать частью любого законодательства по защите детей в киберпространстве. Учитывая международную природу киберпреступности и, особенно, эксплуатации детей, эффективное международное сотрудничество органов охраны правопорядка является необходимым, если мы собираемся решать эту проблему в международном масштабе.

[19] ИНТЕРПОЛ также координирует рабочую группу ИНТЕРПОЛА по преступлениям против детей, которая собирается раз в год. Рабочая группа состоит их пяти подгрупп, и члены этой группы встречаются на протяжении практически всего года, осуществляя работу над проектами. Эти пять подгрупп следующие: преступления против детей, осуществляемые с использованием интернета сексуальные преступления, торговля детьми, а также особо серьезные и жестокие преступления против детей. Пятая подгруппа – это подгруппа по идентификации жертв, которое упрощает международное сотрудничество, которое ведется ежедневно с использованием Международной базы данных сексуальной эксплуатации детей.

Требования к отчетности

Рядовые члены общества, вступившие в контакт с материалами CAM, должны сообщить об этом в местные органы охраны правопорядка и/или по национальной горячей линии[20]. Кроме того, существует три класса частных лиц и организаций, которым следует особенно сообщать о материалах, которые вызывают подозрение о том, что могут быть материалами CAM, либо непосредственно в органы охраны правопорядка, либо в другую уполномоченную организацию, такую как горячая линия:

1 Люди, которые по своей профессиональной деятельности контактируют с детьми и обязаны осуществлять ежедневную заботу о детях, например, учителя, тренеры, консультанты, работники здравоохранения и офицеры органов охраны правопорядка.

2 Люди, которые по своей профессиональной деятельности не обязательно контактирует с детьми, но могут столкнуться с материалами CAM в процессе работы, например, технические специалисты по компьютерам, работники службы проявки фотографий.

3 Организации или корпорации, чьи услуги используются для распространения материалов CAM и которые должны нести корпоративную гражданскую ответственность, например, ISP и поставщики других электронных услуг (ESP), компании, обслуживающие кредитные карты и банки.

Тогда как включение в этот список людей категорий 1 и 2 не требует пояснений, отчетность со стороны ISP, банков и компаний, обслуживающих кредитные карты, очень важна в том смысле, что услуги очень необходимы для передачи таких материалов, и их услуги используются преступниками "не по назначению" для преступлений против детей. Эти отрасли в состоянии обнаруживать доказательства наличия материалов CAM, и их следует активно привлекать к сотрудничеству с властями и предоставлять информацию относительно материалов CAM, когда они обнаружат их.

Следует отметить, что в настоящее время некоторые компании оказывают значительную помощь такого рода. Что касается ISP и ESP, они вероятнее всего могут наткнуться на доказательства наличия материалов CAM в файлах, URL, именах доменов и реальных изображениях, о которых следует немедленно сообщить в соответствующие органы. Более того, сообщения об URL, именах доменов и IP-адресах дают возможность закрыть доступ к известным веб-сайтам с материалами жестокого обращения с детьми. ISP и ESP следует активно призывать проводить упреждающие проверки своих сетей на предмет наличия материалов CAM и сообщать о них в соответствующие органы охраны правопорядка. Учитывая современную роль интернета и его использования в преступных целях, сотрудничество с интернет-компаниями является очень важным. Более того, законодательство должно обеспечить защиту для ISP, ESP и других частных компаний, которые сообщают о материалах CAM, и должно содержать указания по безопасной обработке и передаче изображений.

Должен быть установлен режим "Уведомление и отключение", который позволяет ISP, ESP, регистраторам доменов и сервисам веб-хостинга по запросу закрывать преступные сайты или учетные записи электронной почты. В большинстве случаев такое преступное использование является нарушением соглашений об "Условиях использо-

[20] Национальные горячие линии будут сообщать в органы охраны правопорядка; и органы охраны правопорядка смогут затем проанализировать отчеты по местным связям или передать информацию для анализа в Международную базу данных сексуальной эксплуатации детей.

вания", которые пользователь подписывает с ISP или ESP, давая таким образом компании неоспоримые права предпринимать необходимые действия. По возможности, эти действия должны быть тесно скоординированы с органами охраны правопорядка в целях обеспечения того, что будет организовано расследование, которое может не допустить жестокого обращения с ребенком и обеспечить поимку вовлеченных преступников.

К несчастью, продажа материалов CAM в интернете стала прибыльным глобальным бизнесом, который опирается на услуги банков, телеграфные переводы и кредитные карты, что упрощает продажу, распространение или передачу материалов CAM. Чиновники финансовых организаций, которым встретится информация, относящаяся к CAM, должны сообщить об этом в соответствующие органы. Зачастую веб-сайты, предлагающие материалы CAM в режиме "плата за просмотр" или на основе абонентской платы, принимают к оплате кредитные карты или пользуются услугами перевода денег.

Общим правилом должно быть то, что отрасль финансовых услуг следует призывать к сотрудничеству в соответствии с моделью Финансовой коалиции против детской порнографии (FCACP)[21] – совместного проекта ICMEC и его родственной организацией Национального центра по пропавшим и эксплуатируемым детям (NCMEC). Эта эффективная коалиция создает механизм для тесного сотрудничества служб финансовой отрасли, служб отрасли интернета, органов охраны правопорядка и неправительственных организаций (НПО). Она достигла заметного успеха в прекращении коммерческой поставки материалов CAM и использованием международной финансовой системы. Работая вместе, участники FCACP имеют возможность не только сообщать о подозрительных транзакциях и счетах, но также и отслеживать действия по счету и денежные потоки, для того чтобы идентифицировать людей и организации, которые в конечном итоге ответственны за продажу материалов CAM. Европейский вариант такой коалиции начал работу в 2009 году.

Уменьшение доступности изображений жестокого обращения с детьми

Распространение материалов CAM в интернете вызвало громкие призывы общественности к действию. Органы охраны правопорядка, ISP, ESP и НПО всего мира сотрудничают в борьбе с этим онлайновым контентом. Ясно, что органы охраны правопорядка сами не могут остановить это распространение и что гораздо больше необходимо сделать, для того чтобы прекратить и сократить трафик материалов CAM. В результате, многие страны начали изучать дополнительные средства, которые усиливают традиционные действия, предпринимаемые органами охраны правопорядка.

Подход, принятый в нескольких странах, состоит в том, чтобы призывать ISP и ESP, уменьшать доступность веб-страниц, о которых известно, что они содержат материалы CAM, и блокировать доступ к новостным группам Usenet, которые либо регулярно содержат такой контент, либо рекламируют его доступность.

При таком подходе поставщикам услуг ISP и ESP предоставляется "список" новостных групп и действующих веб-страниц, содержащих или рекламирующих CAM. Этот список составляется либо органами охраны правопорядка, либо, в некоторых случаях, непосредственно национальными горячими линиями. Очень важно, чтобы принципы, на основании которых составляются такие списки, были бы ясно оговорены.

[21] FCACP : http://www.icmec.org/missingkids/servlet/PageServlet?LanguageCountry=en_X1&PageId=3064.

Не должно оставаться возможности для подозрений в том, что правительственные организации, органы охраны правопорядка или иные организации имеют возможность влиять на его создание таким образом, чтобы включать в него новостные группы или веб-сайты, не содержащие материалов САМ, но содержащие материалы, которые для этих организаций нежелательно публиковать по другим причинам.

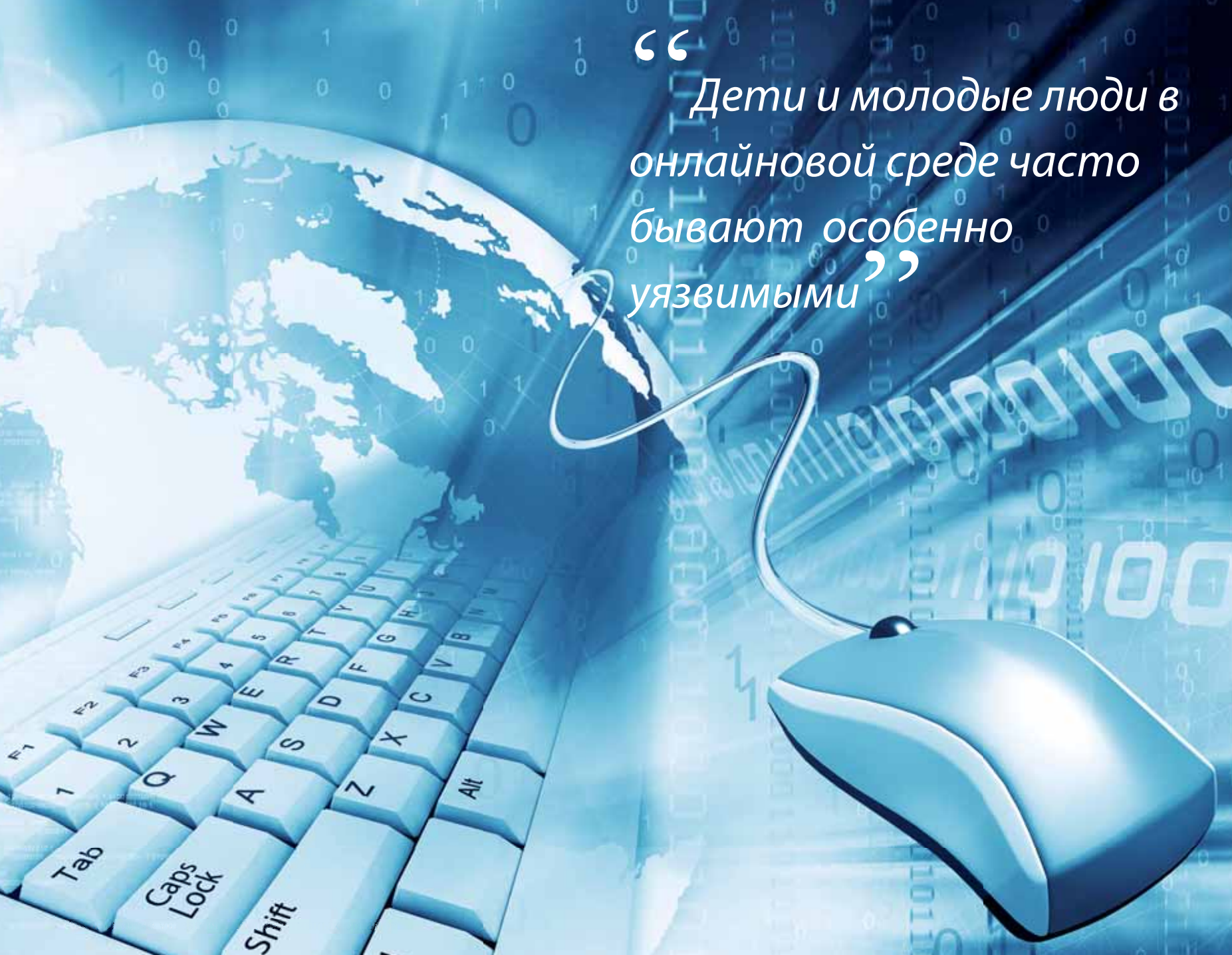
При создании и распространении списка среди ISP и ESP очень важен диалог с органами охраны правопорядка. Органам охраны правопорядка требуется определенное время для получения доступа, просмотра и документирования контента, и, при необходимости, для начала расследования. Если органы охраны правопорядка не смогут выполнить необходимые действия, это может помешать расследованию или затянуть его. Кроме того, без участия органов охраны правопорядка и без расследования, те, кто постоянно распространяет материалы САМ в онлайновом режиме, никогда не будут задержаны и привлечены к ответственности.

Для того чтобы обеспечить точность данных, важно чтобы список известных сайтов и новостных групп Usenet регулярно проверялся, обновлялся и подтверждался. Этот список не должен быть накопительным; наоборот, многоуровневая процедура повторных проверок поможет обеспечить всеобщее доверие к использованию этого списка. Кроме того, важно обеспечить такое положение дел, при котором руководящие указания по критериям этого списка были бы прозрачными. В некоторых странах используются независимые средства проверки характеристик и использования этого списка. И наконец, должен существовать механизм, позволяющий апеллировать против включения в список. В этом списке должны быть перечислены только те сайты, которые разрешают публикацию или воспроизведение контента, который является незаконным в соответствии с национальными законами рассматриваемой страны.

Когда сайт заблокирован, пользователь должен видеть страницу STOP. Эта страница STOP выполняет двойную задачу: предоставляет информацию о причине, по которой был заблокирован сайт (незаконность контента) плюс действует как превентивная мера, напоминая пользователем/потребителям о незаконности материала, а также о присутствии органов охраны правопорядка в онлайновом режиме.

Блокировка доступа к веб-сайтам и новостным группам Usenet, содержащим материалы САМ, может стать важным вкладом в разрушение и уменьшение объемов контента, циркулирующего и распространяемого в интернете. Однако следует понимать, что это только часть решения. Этот подход не является единственным решением. Цель состоит в дополнении действий органов охраны правопорядка и в уменьшении доступности материалов САМ в онлайновом режиме. Люди, имеющие сексуальные интересы в отношении детей и обладающие достаточными техническим знаниями и настойчивостью, могут все же получить возможность найти такие материалы. Однако технология веб, в частности, имеет настолько простой интерфейс пользователя и стала одним из наиболее широко используемых интернет-приложений, что очень важно разработать специальные подходы ее применения, при этом продолжая разработку новых методов препятствования распространению таких материалов на других платформах интернета.

Всегда необходимо помнить о совместных информационных кампаниях правительства/отрасли по повышению осведомленности, направленных на потребителей материалов САМ. Пользователям/потребителям необходимо напоминать, что материалы САМ представляют собой страдания реальных детей, а создание, владение или распространение материалов САМ является незаконным во многих странах.


“Дети и молодые люди в онлайновой среде часто бывают особенно уязвимыми”

4. Основные риски для детей в онлайновой среде

Хотя взрослые и дети одинаково подвергаются различным рискам в онлайновой среде, дети и молодые люди часто особенно уязвимы. Дети еще находятся в процессе развития и обучения. Это имеет свои последствия для их возможности идентифицировать, оценивать и контролировать возможные риски. Мысль о том, что дети уязвимы и их следует защищать от всех форм эксплуатации, определена в Конвенции ООН по правам ребенка[22].

Существует множество проблем, связанных с использованием интернета детьми и молодыми людьми, которые постоянно беспокоят как родителей, так и детей, а также правительства, политиков и директивные органы. Области этой озабоченности можно сформулировать следующим образом:

Контент

- Возможность интернета подвергать детей и молодых людей воздействию незаконного контента, например, материалов САМ.
- Возможность интернета подвергать детей и несовершеннолетних молодых людей воздействию непригодных для них материалов, например жестоких изображений.

Контакты

- Возможность интернета подвергать детей и несовершеннолетних возможному влиянию со стороны сексуальных интернет-хищников, вне зависимости от того являются ли они взрослыми или несовершеннолетними[23].

[22] http://www.unhchr.ch/html/menu3/b/k2crc.htm

[23] Этот аспект подробно рассматривается в Приложении 1.

- Способ, при помощи которого интернет может подвергать детей влиянию вредных онлайновых сообществ, например, сайтов, поощряющих анорексию, самоистязание или самоубийства, а также источников политического влияния, пропагандирующих жестокость, ненависть и политический экстремизм.

Поведение

- Способ, при помощи которого интернет содействует и может продвигать рискованные сексуальные взаимоотношения между самими детьми, включая поощрение их создавать и размещать собственные изображения или изображения других людей (секстинг), которые помимо того что являются вредными, еще и незаконны. Нормальное сексуальное развитие и онлайновые эксперименты могут иногда привести к неумышленному созданию и распространению материалов САМ, подвергающих ребенка и его или ее друзей возможным правовым санкциям или привлечению к ответственности в системе уголовного права.
- Способ, при помощи которого некоторые аспекты интернета поощряют детей к размещению в открытом доступе информации о себе или размещению фотографий или видеороликов или текстов, которые могли бы повредить их личной безопасности или разрушить многие возможности для их профессиональной карьеры в будущем.
- Возможность интернета подвергать детей и молодых людей запугиванию и допускать существование или пропагандировать условия, в которых поощряются запугивание других людей со стороны детей и молодых людей.

Торговля

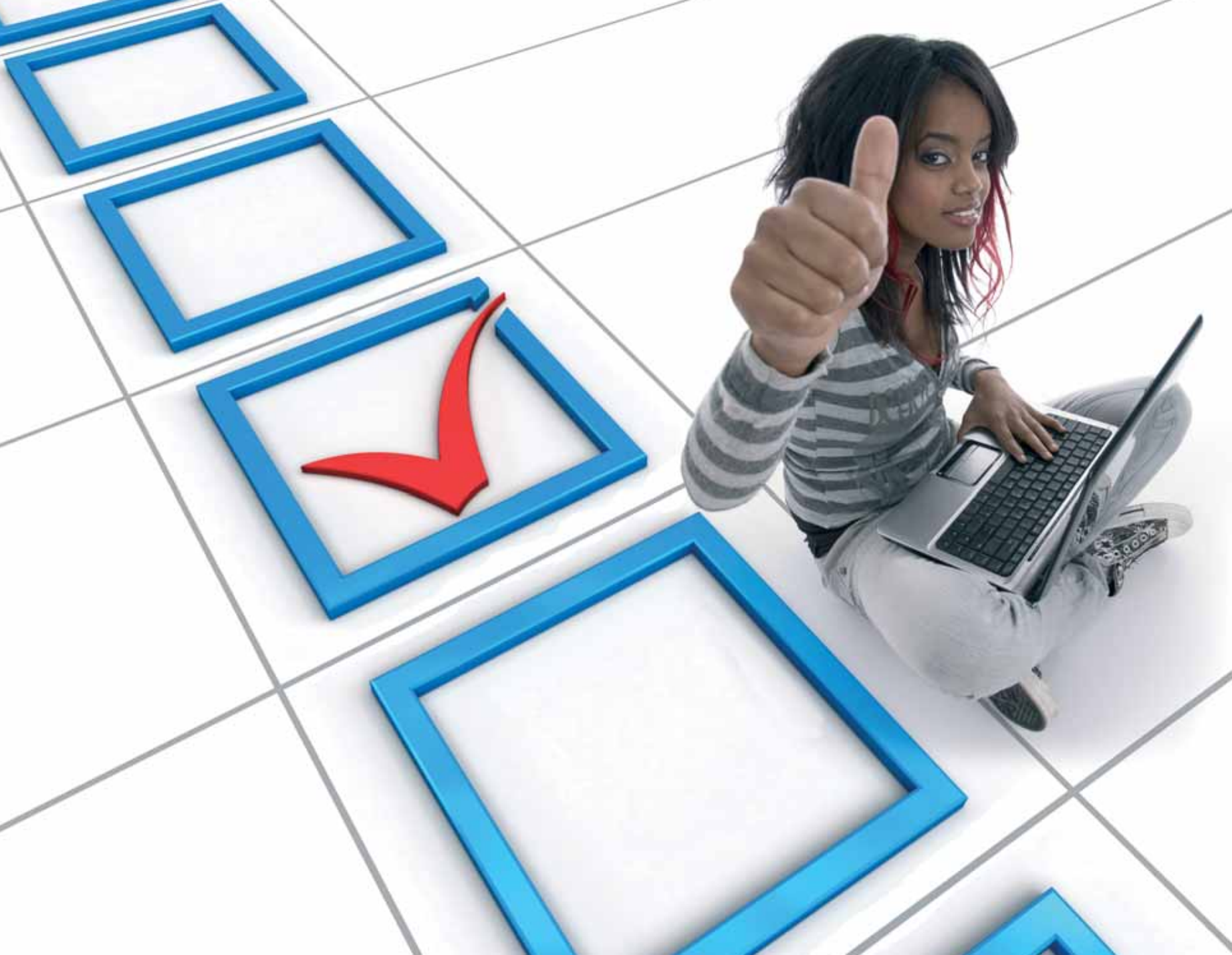
- Способы, при помощи которых интернет дает детям возможность получить доступ и приобрести неподобающие их возрасту товары и услуги, как правило, товары и услуги, которые они не могут купить лично в магазине.
- Возможность интернета подвергать детей и молодых людей риску обмана, кражи идентичности, мошенничества и аналогичных угроз, которые имеют экономическую природу и обусловлены недостатками законов о защите информации или конфиденциальности.

Чрезмерное использование

- Способ, при помощи которого интернет, как кажется некоторым детям и молодым людям, стимулирует виды навязчивого поведения или чрезмерного использования, которые могут иметь пагубные последствия для здоровья или социальных навыков детей и молодых людей, или для того и другого одновременно. Компьютерные игры и игра в них по интернету часто формируют такой тип онлайнового поведения, которое в некоторых странах считается одной из форм зависимости.

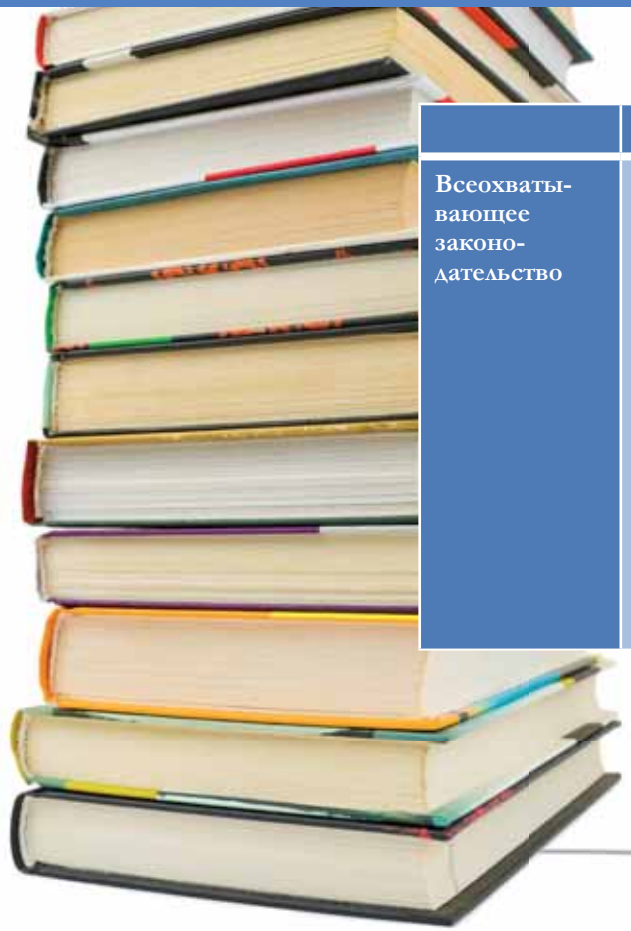
Общественная жизнь

- Способ, при помощи которого интернет создает новый цифровой разрыв между детьми и молодыми людьми, как в том, что одни из них имеют простой и удобный доступ к интернету дома, в школе и где угодно, а другие такого доступа не имеют; так и в том, что одни из них являются уверенными и умелыми пользователями, а другие таковыми не являются. Этот разрыв угрожает укрепить и или расширить существующие шаблоны преимуществ и недостатков или, возможно, создать новые разрывы.
- Потенциальная возможность интернета усугубить и даже увеличить существующую уязвимость особых групп детей и молодых людей, что добавится к тем неблагоприятным факторам, с которыми они сталкиваются в реальном мире.



5. Решение проблем с рисками

Список для самопроверки на национальном уровне



	№	Список для самопроверки на национальном уровне
Всеохватывающее законодательство	1	Как правило, потребуется введение блока законов, которые разъясняют, что любое и каждое преступление, которое может быть совершено против ребенка в реальном мире, может, *с учетом соответствующих поправок,* также быть совершено в интернете или любой другой электронной сети. Кроме того, может потребоваться разработать новые или пересмотреть существующие законы, для того чтобы установить незаконность определенных видов поведения, которые могут существовать только в интернете, например, дистанционное заманивание детей для выполнения и просмотра сексуальных действий, или "соблазнение" детей для встречи в реальном мире с сексуальными целями. В дополнение к этим целям, как правило, потребуется ввести законодательство, которое установит незаконность злонамеренного использования компьютеров в преступных целях, незаконность хакерства и другого вредоносного и несоответствующего использования компьютерных программ, и определит, что интернет является местом, в котором могут быть совершены преступления.

	№	Список для самопроверки на национальном уровне
Потребность учета национальных особенностей в защите ребенка в онлайновой среде	2	Некоторые национальные правительства нашли полезным свести воедино все заинтересованные стороны и участников рынка для разработки и реализации национальной инициативы с целью сделать интернет более безопасным местом для детей и молодых людей, а также с целью повышения осведомленности о проблемах и о том, как их решать на практике. В рамках этой стратегии важно понимать, что сегодня доступ в интернет можно получить с использованием различных видов устройств. Компьютеры – это только один из способов выйти в он-лайн. Мобильные телефоны, игровые консоли и PDA также используются все чаще. В работе должны участвовать поставщики услуг как беспроводного, так и фиксированного доступа. Кроме того, во многих странах важным источником доступа в интернет, особенно для детей и молодых людей, является сеть общественных библиотек, центров связи и интернет-кафе. Некоторые страны для разработки правил в этой области нашли полезным создать модель самостоятельного или совместного регулирования, и при помощи таких моделей они, например, публикуют кодексы добросоветской практики, с тем чтобы направлять отрасль интернет, используя те меры, которые могут наилучшим образом работать там, где дело касается обеспечения безопасности детей и молодых людей в онлайновой среде. Такой подход работает также и на региональном уровне, например, в рамках Европейского союза, где опубликованы кодексы ЕС, как для сайтов общения в социальных сетях, так и для сетей мобильной телефонии, связанные с поставкой контента и услуг детям и молодым людям по этим сетям. Самостоятельное или совместное регулирование может быть очень эффективным способом содействия в привлечении и поддержании вовлеченности всех соответствующих заинтересованных участников и может быть очень эффективным в том, что касается повышения скорости, с которой могут быть сформулированы и введены в действия соответствующие меры реакции на технологические изменения. Школы и система образования, как правило, играют важную роль в развертывании такой национальной стратегии, но эта стратегия также должна быть намного шире.

	№	Список для самопроверки на национальном уровне
Потребность учета национальных особенностей в защите ребенка в онлайновой среде		Следует также рассмотреть вопрос помощи со стороны средств массовой информации в распространении данных и проведении кампаний с целью повышения осведомленности.
Потребность создания местных ресурсов, которые отражают национальные законы и местные культурные нормы	3	Множество крупных интернет-компаний создают веб-сайты, содержащие большой объем информации об онлайновых угрозах для детей и молодых людей. Однако очень часто этот материал доступен только на английском языке или на небольшом числе языков. Следовательно, очень важно, чтобы материалы создавались на местах и отражали национальные законы и местные культурные нормы. Это будет важно для любой кампании по безопасности интернета и для разработки любых обучающих материалов.
Потребность в действиях по обучению населения и повышения осведомленности	4	Родители, опекуны и люди таких профессий как учителя, играют важнейшую роль в том, чтобы помогать детям и молодым людям оставаться в безопасности, находясь в он-лайне. Должны быть разработаны образовательные и информационно-пропагандистские программы, которые позволят обеспечить осведомленность по этим проблемам, а также определят стратегию борьбы с ними. При создании обучающих материалов важно учитывать, что многие люди, мало знающие о технологии, будут чувствовать себя не очень удобно, используя ее. По этой причине важно обеспечить, чтобы материалы о безопасности были доступны как в напечатанном виде, так и при помощи других средств информации, с которыми новички будут чувствовать себя более комфортабельно, например, в виде видеороликов. В рамках многих образовательных и информационных кампаний важно выбрать правильный тон. Следует избегать пугающих сообщений, и поэтому акцент должен быть сделан на многие положительные и развлекательные возможности новых технологий. Интернет имеет огромный потенциал как средство помощи детям и молодым людям в исследовании новых миров. Обучение их позитивным и ответственным формам онлайнового поведения является главной задачей образовательных и информационных программ.

	№	Список для самопроверки на национальном уровне
Потребность в механизмах сообщения о преступном поведении в он-лайне, включая запугивание	5	Механизмы для сообщения о злонамеренном использовании онлайновых услуг или для сообщения о неприемлемом или незаконном поведении в он-лайне, например, по национальной горячей линии, следует широко рекламировать и продвигать как в интернете, так и в других средствах информации. Ссылки на механизмы для сообщения о злонамеренном использовании должны быть явно отображены на соответствующих участках каждого веб-сайта, которые позволяют размещать контент, создаваемый пользователями. Должна быть также обеспечена возможность, чтобы люди, которые чувствуют, что им грозит опасность любого вида, или люди, заметившие любые подозрительные действия в интернете, могли бы максимально быстро сообщить в соответствующие органы охраны правопорядка, которые должны быть обучены и готовы среагировать на это заявление. Виртуальная глобальная целевая группа – это организация органов охраны правопорядка, которая предоставляет действующий в режиме 24/7 механизм для принятия от граждан США, Канады, Австралии и Италии заявлений о незаконном поведении или контенте, ожидается, что другие страны также присоединятся. См. www.virtualglobaltaskforce.com
Способствуя большей безопасности детей путем применения технических средств	6	Существует множество доступных программ, которые помогают выявить нежелательные материалы или заблокировать нежелательные контакты. Некоторые из этих программ обеспечения безопасности ребенка и фильтрующих программ могут быть совершенно бесплатными, поскольку они входят в состав операционной системы компьютера, или они поставляются как часть пакета услуг ISP или ESP. Производители некоторых игровых консолей также предоставляют аналогичные инструменты, если устройство допускает выход в интернет. Эти программы не являются гарантией полной защиты, но они могут обеспечить хороший уровень поддержки, особенно в семьях с маленькими детьми. Эти технические инструменты следует использовать как часть более обширного арсенала. Очень важно участие родителей и/или опекунов. Когда дети взрослеют, они потребуют больше конфиденциальности и также ощутят сильное желание начать собственные исследования. Кроме того, там где между продавцом и потребителем существуют финансовые отношения, очень ценную помощь может оказать процесс подтверждения возраста, помогающий продавцам товаров и услуг, имеющих возрастные ограничения, а также издателям материалов, предназначенных только для читателей старше определенного возраста, иметь доступ к этой специфической аудитории. Там, где финансовых отношений нет, использование технологий подтверждения возраста может оказаться проблематичным, или во многих странах оно может оказаться невозможным из-за отсутствия надежных источников данных.

Руководящие указания для директивных органов

6. Заинтересованные стороны

При разработке национальной стратегии обеспечения онлайновой безопасности для детей и молодых людей, национальные правительства и директивные органы должны определить основные заинтересованные стороны и привлечь их к работе.

Дети и молодые люди

Во всем мире дети и молодые люди продемонстрировали, что они очень легко могут адаптироваться к новым технологиям и использовать их. Интернет становится все более значимым в школах в качестве среды, в которой дети и молодые люди работают, играют и общаются.

Большая часть детей и молодых людей не испытывают страха перед интернетом и с удобством используют различные устройства, которые дают сегодня возможность доступа к нему. Знания детей и молодых людей о том, как работают компьютеры и интернет, часто превосходят знания родителей и учителей в этой области.

Но знания – это не мудрость. Нехватка у детей и молодых людей опыта существования в мире может оставлять их уязвимыми для широкого диапазона рисков. Они имеют право ждать помощи и защиты. Важно также напомнить, что не все дети и молодые люди будут одинаково использовать интернет или новые технологии. Некоторые дети с особыми потребностями, обусловленными ограничениями физических или других возможностей, могут оказаться особенно уязвимыми в онлайновой среде и, следовательно, будут нуждаться в дополнительной поддержке.

Обзоры постоянно показывают: то, что думают взрослые о том, что дети и молодые люди делают в он-лайне, и то, что там происходит на самом деле, – может совершенно не совпадать. По этой причине, если нет других

причин, важно обеспечить при любых мероприятиях на национальном уровне по разработке правил для этой области, чтобы были найдены соответствующие механизмы, которые позволят услышать голоса всех детей и молодых людей и учесть их конкретный опыт использования технологии.

Родители, опекуны и учителя

Одна из причин, по которым многие родители покупают компьютеры с доступом в интернет для домашнего использования, – это помощь в образовании их детей и в выполнении домашних заданий. Следовательно, школы несут особую ответственность за то, чтобы научить детей тому, как оставаться в безопасности в он-лайне, вне зависимости от того, используют ли они интернет в школе, дома или где-либо еще. Для того чтобы учителя могли это сделать, им, в свою очередь, нужен профессиональный тренинг, связанный с первоклассными современными обучающими ресурсами.

Родители и опекуны почти всегда будут первой, последней и лучшей линией защиты и поддержки своих детей. Однако когда дело касается интернета, они могут чувствовать себя несколько растерянными. Опять же, школы могут действовать как важный канал связи с родителями и опекунами, сообщая им как про риски, так и про множество положительных возможностей, предоставляемых новыми технологиями. Однако школы не должны стать единственным способом, используемым для информирования родителей и опекунов. Важно использовать множество различных каналов, для того чтобы обеспечить максимальную вероятность информирования максимально возможного числа родителей и опекунов. Общественные библиотеки, медицинские центры, даже торговые центры – все могут предоставить доступные места для представления информации о безопасности.

Отрасль

Очевидно, что компании, которые разрабатывают или поставляют продукты и услуги новых технологий, будут иметь хорошую возможность оказания помощи другим заинтересованным сторонам в понимании того, как они работают и как их использовать безопасно и надлежащим образом. По этой причине важно проводить работу с предприятиями и поощрять распространение ими информации и знаний.

Кроме того, отрасль несет основную ответственность за содействие повышению информированности, в частности, детей и молодых людей, а также их родителей или опекунов, и, кроме того, широкой общественности о правилах работы в он-лайне и правилах безопасности. Участвуя в процессе, таким образом, отрасль узнает больше об опасениях различных заинтересованных участников, и это знание поможет им определить такие угрозы в любых новых продуктах или услугах, которые он разрабатывают, а также помогут им скорректировать существующие.

В некоторых странах интернет регулируется на основе самостоятельного или совместного регулирования. Это может дать отрасли интернета право голоса в ходе разработки общественных правил и может помочь в обеспечении того, чтобы эти правила были хорошо обоснованы технически. Это означает также, что с изменением технологии, изменения в практическом применении будут вноситься достаточно быстро, не ожидая завершения иногда продолжительных процессов, необходимых для разработки и введения новых законов. В то время как привлечение отрасли помогает достичь лучшего понимания проблем онлайновой безопасности, для национальных правительств и других органов директивного сообщества также важно иметь собственных независимых источников для консультаций.

Научно-исследовательское сообщество и НПО

Вполне возможно, что в университетах и других составляющих научно-исследовательского сообщества есть множество ученых и студентов, имеющих профессиональный интерес и очень хорошие знания, как об общественных, так и о технических аспектах и воздействии интернета. Они могли бы стать очень ценным ресурсом в деле оказания помощи национальным правительствам и директивным органам в разработке стратегий, которые были бы основаны на твердо установленных фактах и надежных доказательствах. Они также могут действовать в качестве интеллектуального противовеса высокотехнологичным компаниям, интересы которых могут иногда быть краткосрочными по своей природе и, главным образом, иметь коммерческий характер.

Подобным образом в неправительственных организациях очень часто можно найти широкий спектр профессиональных знаний и опыта, которые могут стать бесценным ресурсом для информирования или предоставления услуг детям, молодым людям, родителям, опекунам и учителям, помогая выполнять план действий по онлайновой безопасности.

Органы охраны правопорядка

Очень печально, что такая замечательная технология привлекает также внимание криминальных и антисоциальных элементов. Интернет значительно повысил объемы циркуляции материалов CAM. Сексуальные интернет-хищники используют интернет для знакомства с детьми и молодыми людьми, заманивая их участвовать в очень опасных формах контактов в онлайне и в реальном мире. Запугивание и другие формы преследования могут причинить большой вред жизни детей и молодых людей, и интернет позволил сделать это совершенно по-другому.

По этим причинам важно, чтобы органы охраны правопорядка полностью занимались бы деятельностью, связанной с любой общей стратегией, с тем чтобы помочь сделать интернет более безопасным для детей и молодых людей. Сотрудники органов охраны правопорядка должны быть соответствующим образом обучены ведению следствия по совершенным с помощью интернета преступлениям против детей и молодых людей. Им нужно обладать нужным уровнем технических знаний и доступом к средствам криминалистики, которые дали бы им возможность получать данные из компьютеров или интернета и интерпретировать их.

Кроме того, очень важно, чтобы органы охраны правопорядка сформировали ясные механизмы, позволяющие детям и молодым людям или любому другому гражданину сообщать о любых происшествиях или опасениях, которые могут у них возникнуть относительно безопасности ребенка или подростка в онлайновой среде. Во многих странах, например, созданы горячие линии для упрощения передачи сообщений о материалах CAM, и существуют аналогичные специальные механизмы для упрощения передачи сообщений по любым типам проблем, например, о запугивании и других типах угрожающего поведения.

Органы охраны правопорядка являются главным источником по сбору CAM в пределах национальных границ. Необходимо организовать процесс по изучению этих материалов, для того чтобы установить, могут ли быть идентифицированы местные жертвы.Там, где это невозможно, материалы следует передать в Интерпол для включения в базу данных ICSE.

Социальные службы

Там, где дети или молодые люди испытывали вредные воздействия или жестокое обращение в онлайновом режиме, например, если в сети были размещены неприемлемые или незаконные их изображения, вполне вероятно, что им требуется специализированная и долгосрочная поддержка или консультация. Профессионалы, работающие в социальных службах, должны быть соответствующим образом обучены, для того чтобы иметь возможность предоставить поддержку такого вида.

7. Вывод

Интернет сегодня стал незаменимым связующим звеном для множества цифровых технологий, которые изменяют экономику, открывая массу возможностей по улучшению качества жизни людей и обогащения общества разнообразными способами.

На макроуровне чрезвычайно важно, чтобы экономические преимущества, которые может создать интернет, равномерно распространялись по всему миру. Вероятность роста цифрового разрыва между развитым миром и развивающимися в промышленном отношении странами, расширяющего или увеличивающего существующие недостатки или диспропорции, рассматривалась в ходе ВВУИО. Она продолжает оставаться главным вопросом политических дискуссий на форуме ВВУИО[24], Форуме регулирования интернета (IGF)[25] и на многих соответствующих международных форумах.

На уровне отдельного пользователя интернет стал технологией, дающей существенные преимущества и возможности. Преимущества интернета и связанных с ним цифровых технологий особенно заметны детям и молодым людям. Эти технологии изменяют способ нашего общения друг с другом и открыли множество новых путей для игр, прослушивания музыки и участия в разнообразных культурных мероприятиях, разрушив многочисленные барьеры во времени и в пространстве. Дети и молодые люди зачастую находятся на

[24] http://www.itu.int/wsis/implementation/2009/forum/geneva/index.html

[25] www.intgovforum.org

переднем крае, где принимают возможности, предоставляемые интернетом, и приспосабливаются к ним.

Конечно, нельзя отрицать, что как следствие появления интернета, появилось множество задач по обеспечению безопасности детей и молодых людей, которые требуется решать, как потому, что это полагается по праву его существования, так и потому что важно донести до всех опасающихся, что интернет является той средой, которой мы все должны уметь доверять. Точно также важно, чтобы мы все вместе не допустили того, что явное беспокойство по поводу защиты детей и молодых людей в онлайновой среде стало платформой для оправдания полностью беспочвенных обвинений в нарушении свободы речи, свободы самовыражения и свободы собраний.

Чрезвычайно важно, чтобы следующее поколение могло уверенно использовать интернет, для того чтобы они могли, в свою очередь, продолжать пользоваться преимуществами его развития. Таким образом, при рассмотрении безопасности детей и молодых людей в онлайновом режиме, очень важно найти золотую середину.

Очень важно открыто обсуждать опасности, существующие для детей и молодых людей в онлайновом режиме, так чтобы мы могли бы научить их, как полностью избегать рисков или научить, как бороться с ними, если они, тем не менее, возникают, однако, мы должны делать это так, чтобы не преувеличивать опасности и не слишком испугать их. Маловероятно, что подход, в котором учитываются только негативные аспекты технологии, либо главным образом негативные аспекты, будет всерьез принят детьми и молодыми людьми, потому что сотни миллионов их уже используют ее каждый день, и, следовательно, они очень много знают о том, что это такое и чем это может быть. В этой связи родители и люди старших поколений могут часто считать себя в проигрыше. Например, когда молодые люди очень часто знают о технологии и ее возможностях больше, чем их родители и учителя. Но знания – это не то же самое, что мудрость.

Национальные правительства обязаны обеспечить защиту несовершеннолетних как в "реальном", так и в "виртуальном" мирах. Важно, что поскольку сейчас новые технологии так хорошо интегрированы в жизнь такого большого числа детей и молодых людей по ряду важных направлений, более не имеет смысла пытаться сохранять четкое различие между событиями "реального мира" и онлайновым событиями. Они все больше пересекаются и все больше зависят друг от друга.

Национальные правительства и директивные органы несут основную ответственность как за создание базы, на основе которой могут быть разработаны соответствующие национальные и многонациональные меры реагирования, так и за поддерживание ее существования в дальнейшем. В этом процессе как сама отрасль интернета, так и соответствующие заинтересованные стороны будут играть очень важные роли, потому что скорость изменения технологии означает, что многие традиционные методы разработки законов или правил более не отвечают этой цели. Как показывает этот отчет, новые технологии выдвигают также и новые требования к лицам, занимающимся законотворчеством.

Приложение 1

Контактные преступления против детей и молодых людей

Дети и молодые люди могут быть открыты для многочисленных нежелательных и неподобающих контактов в интернете, которые могут иметь роковые последствия для них. Некоторые их этих контактов могут иметь сексуальную природу.

Исследования, проведенные в Европе компанией Kids Online в 2008 году, выявили некоторые тревожные результаты (усредненные данные): 15–20% испытывают запугивание, домогательства или преследование в онлайновом режиме; 25% получают нежелательные сексуальные комментарии; 9% встречались в реальной жизни с людьми, с которыми до этого общались только в он-лайне. Хотя значения для разных стран и разных регионов разные, эти цифры показывают, что риски являются реальными[26] . В одном американском исследовании интернета[27] отмечено, что 32% подростков общались с совершенно незнакомым человеком, 23% из них сказали, что им было страшно и неудобно во время беседы; и 4% этих детей говорят о настойчивых и агрессивных сексуальных приставаниях.

Сексуальные интернет-хищники используют интернет для общения с детьми и молодыми людьми с сексуальными целями, часто используя приемы, известные под названием "груминг", при помощи которых они добиваются доверия ребенка, обращаясь к его или ее интересам. Они часто вводят сексуальные темы, фотографии и откровенные языковые средства, для того чтобы уменьшить восприимчивость, повысить сексуальную осведомленность и смягчить волю своих маленьких жертв. Подарки, деньги и даже билеты на транспорт используются для того, чтобы уговорить ребенка или молодого человека и заманить его в то место, где интернет-хищник может сексуально эксплуатировать его или ее. Эти встречи могут даже фотографироваться или вестись их видеозапись. Детям и молодым людям часто не хватает эмоциональной зрелости и чувства собственного достоинства, что делает их уязвимыми для манипуляций и запугивания. Они также боятся сказать взрослым о своих встречах, опасаясь попасть в неловкое положение или потерять доступ к интернету. В некоторых случаях им угрожает интернет-хищник и заставляет держать их отношения в тайне.

Сексуальные интернет-хищники учатся друг у друга в интернет-форумах и в чатах. Общаясь с детьми и молодежью, эти интернет-хищники часто делают вид, что они почти того же возраста, что и ребенок или молодой человек, то есть моложе, чем они есть на самом деле, и претендуют на то, что ищут друга. Как только они добились доверия ребенка, они пользуются его уязвимыми точками, например, одиночеством или потрясением из-за личной потери, для создания эмоциональной зависимости от интернет-хищника. В средствах массовой информации имеется множество сообщений о случаях, когда ребенок или молодой человек соглашались на личную встречу с кем-то, с кем общались только в он-лайне, и

[26] EU Kids Online Report, Comparing Children's Online Opportunities and Risks Across Europe, pages 29- 30, June 2008.

[27] Pew Internet and American Life Project 2007.

кто, по их мнению, был человеком его возрастной группы, и обнаруживали, что это пожилой мужчина, заинтересованный в сексуальных отношениях с ними. К несчастью, некоторые из этих случаев приводили к насилию над жертвой и сексуальным действиям с ребенком; в ряде случаев последствия были еще хуже.

Особенно беспокоящая тенденция заключается в том, что интернет-хищники распространяют видео с сексуальными действиями над детьми или молодыми людьми, ведя прямую трансляцию видео с вебкамеры, для просмотра другими интернет-хищниками – часто, стремясь заслужить их одобрение. В таких случаях ребенок или молодой человек не только страдает физически и получает психологическую (и иногда физическую) травму в результате этого гнусного действия, но снова и снова становится жертвой в результате передачи этих изображений в интернет, где они становятся объектами коллекционирования другими интернет-хищниками. Эти новые изображения с удовольствием получают и используют, обмениваются ими и иногда продают через интернет другим интернет-хищникам, которым необходим новый материал для удовлетворения их сексуальных фантазий. К сожалению, жертвы зачастую неспособны почувствовать, что все закончилось, и продолжать нормальную жизнь после того, как произошли эти ужасные события, потому что они живут в постоянном страхе от того, что кто-то их узнает на этих их изображениях. Еще более гнусным является использование этих изображений интернет-хищником для шантажа ребенка или молодого человека, заставляя его хранить молчание и продолжая подвергать его жестокому обращению.

Приложение 2

"Детская порнография: Модель законодательства и Глобальный обзор"

При поддержке Интерпола и компании Microsoft, Международный центр по пропавшим без вести и эксплуатируемым детям (ICMEC) сделал обзор законодательства по детской порнографии в 187 странах – членах Интерпола и сформулировал рекомендации по ключевым понятиям, которые при применении в национальном законодательстве составляют всеохватывающую законодательную стратегию борьбы с детской порнографией.

К сожалению, в отчете сделан вывод[28], что только малое число стран мира ввели в действие законодательство, которое достаточно для борьбы с детской порнографией на некотором уровне.

Полный отчет, который сейчас издан уже в 5-м издании, размещен по адресу www.icmec.org на арабском, английском, французском, корейском, португальском, русском, испанском, тайском и турецком языках[29].

Далее приведен список стран – членов Интерпола, и состояние существующего в них законодательства по детской порнографии.

[28] В отчете сделан вывод, что:

- ✓ только в 29 странах имеется законодательство, которое достаточно для борьбы с преступлениями, связанными с детской порнографией (5 стран – членов Интерпола отвечают всем вышеприведенным критериям, и 24 страны – членов Интерпола отвечают всем критериям, за исключением последнего, относящегося к отчетности ISP; и
- ✓ 93 страны – членов Интерпола совсем не имеют законодательства, касающегося специально детской порнографии.

Из оставшихся стран – членов Интерпола, которые имеют законодательство, касающееся специально детской порнографии:

- 54 не определяют детскую порнографию в национальном законодательстве;
- 24 не имеют явных положений о преступлениях, совершенных с использованием компьютеров; и
- 36 не считают преступлением владение материалами детской порнографии, вне зависимости от намерения их распространять.

[29] www.icmec.org

Глобальный обзор

(Перепечатано с разрешения Международного центра по пропавшим без вести и эксплуатируемым детям)

✗ = Нет ✓ = Да

Страна	Специальное законодательство по детской порнографии[30]	Дано определение "Детской порнографии"	Преступления, совершенные с использованием компьютера[31]	Просто владение[32]	Сообщения поставщиков услуг интернета (ISP)[33]
Афганистан	✗	✗	✗	✗	✗
Албания	✗	✗	✗	✗	✗
Алжир	✗	✗	✗	✗	✗
Андорра	✓	✗	✗	✓	✗
Ангола	✗	✗	✗	✗	✗

[30] Для подготовки данного отчета мы искали специализированные законы, которые объявляют вне закона и/или наказывают преступления, связанные с детской порнографией. Обычное законодательство о труде, которое просто запрещает "худшие формы детского труда", в число которых входит детская порнография, не считалось "Специальным законодательством по детской порнографии". Более того, страны, в которых порнография запрещена вообще, вне зависимости от того, являются ли изображаемые люди взрослыми или детьми, также не считались имеющими "Специальное законодательство по детской порнографии", если только в нем не предусмотрено специального наказания за преступления, совершенные против детей.

[31] Для того чтобы квалифицировать преступление как совершенное с использованием компьютера, мы искали специальное упоминание компьютера, компьютерной системы, интернет, или аналогичных слов (даже упоминаний "компьютерных изображений" или чего-либо похожего в определении "детской порнографии"). В тех случаях, когда в национальном законодательстве используются другие слова, приводится поясняющее примечание.

[32] "Простое владение" в тексте данного отчета означает владение вне зависимости от намерения распространять.

[33] Хотя некоторые страны могут иметь общие законы о сообщениях, т. е. любой, кто знает о каком-либо преступлении, должен сообщить о преступлении в соответствующие органы, только те страны, которые специально требуют от ISP сообщать в органы охраны правопорядка (или в другое компетентное ведомство) о случаях подозрений на детскую порнографию, указаны как имеющие законы по "Сообщениям поставщиков услуг интернета (ISP)". Отметим, что в национальных законах (главным образом в странах Европейского союза) имеются также положения, которые ограничивают ответственность ISP, если ISP удалит незаконный контент, как только узнает о нем; однако, такое законодательство в этот раздел не включено.

Страна	Специальное законодательство по детской порнографии	Дано определение "Детской порнографии"	Преступления, совершенные с использованием компьютера	Просто владение	Сообщения поставщиков услуг интернета (ISP)
Антигуа и Барбуды	✗	✗	✗	✗	✗
Аргентина	✓	✓	✓	✗	✗
Армения	✓	✗	✓	✗	✗
Аруба	✓	✗	✓	✓	✗
Австралия	✓	✓	✓	✓	✓
Австрия	✓	✓	✓[34]	✓	✗
Азербайджан	✗	✗	✗	✗	✗
Багамы	✗	✗	✗	✗	✗
Бахрейн	✗	✗	✗	✗	✗
Бангладеш	✗	✗	✗	✗	✗
Барбадос	✓	✗	✗	✓	✗

[34] Раздел 207a(1)(3) Уголовно-процессуального кодекса Австрии квалифицирует как преступление "размещение в общем доступе **любым другим способом**…порнографическое изображение несовершеннолетнего". *Выделение добавлено авторами отчета.*

Страна	Специальное законодательство по детской порнографии	Дано определение "Детской порнографии"	Преступления, совершенные с использованием компьютера	Просто владение	Сообщения поставщиков услуг интернета (ISP)
Беларусь	✓	✗	✗	✗	✗
Бельгия	✓	✓	✓[35]	✓	✓
Белиз	✗	✗	✗	✗	✗
Бенин	✗	✗	✗	✗	✗
Бутан	✓	✗	✓[36]	✗	✗
Боливия	✗	✗	✗	✗	✗
Босния и Герцеговина	✓	✗	✓[37]	✓	✗
Ботсвана	✗	✗	✗	✗	✗
Бразилия	✓	✓	✓	✓	✗

[35] Статья 383bis Уголовно-процессуального кодекса Бельгии в дополнении от 1 апреля 2001 года квалифицирует как преступление, помимо прочего, распространение детской порнографии, включая распространение посредством компьютеров. Письмо от Жана Льюкса (Jan Luykx), заместителя руководителя службы, Посольство Бельгии, Вашингтон, Эмми Ален (Ernie Allen), Президенту и Генеральному директору Международного центра по пропавшим без вести и эксплуатируемым детям (24 февраля 2006 года) в базе данных Международного центра по пропавшим без вести и эксплуатируемым детям.

[36] В соответствии со Статьей 225(b) Уголовно-процессуального кодекса Бутана, "[a] обвиняемый должен быть виновен по обвинению в педофилии, если обвиняемый…продает, производит, распространяет, или еще **каким-нибудь образом взаимодействует** с материалами, которые содержат любое изображение ребенка, вовлеченного в сексуальный контакт". *Выделение добавлено авторами отчета.*

[37] Статьи 189 и 211 Уголовно-процессуального кодекса Боснии и Герцеговины в дополнение к фотографиям и аудиовизуальным записям указывает "другие порнографические материалы".

Страна	Специальное законодательство по детской порнографии	Дано определение "Детской порнографии"	Преступления, совершенные с использованием компьютера	Просто владение	Сообщения поставщиков услуг интернета (ISP)
Бруней	✓	✗	✓	✗	✗[38]
Болгария	✓	✗	✓[39]	✓	✗
Буркина-Фасо	✗	✗	✗	✗	✗
Бурунди	✗	✗	✗	✗	✗
Камбоджа	✗	✗	✗	✗	✗
Камерун	✗	✗	✗	✗	✗

[38] Хотя в законах Брунея нет требования об обязательном сообщении, написанного специально для ISP, поставщики интернет-контента (ICP), имеющие лицензии, соответствующие Классификатору радиовещательных лицензий (Класс лицензий) 2001 года, должны соблюдать Процессуальный кодекс, установленный в Законе о радиовещании (Cap 181). ISP и ICP должны выполнять указания министра, ответственного за вопросы радиовещания, в соответствии с которыми они должны предпринимать ответственные шаги для выполнения этого требования. В соответствии с Законом о радиовещании такой министр имеет право применять санкции. Контент, который не должен разрешаться, включает в себя, помимо прочего, контент, на котором изображается или пропагандируется педофилия.
Лицензиат должен удалить или запретить вещание представленной на его службе программы целиком или ее части, если Министр сообщил Лицензиату, что вещание этой программы целиком или ее части противоречит Процессуальному кодексу, применяемому к этому Лицензиату, или если эта программа противоречит общественным интересам, общественному порядку или национальной гармонии, или нарушает правила хорошего вкуса и приличия. Лицензиат должен также помогать министру, ответственному за вопросы радиовещания, в расследовании любых нарушений своей лицензии или любого нарушения закона, совершенного лицензиатом или любым другим человеком; и должен также формировать такую информацию как записи, документы, данные или другие материалы, которые могут потребоваться министру для целей расследования. Электронное письмо от Сальмы Саллех, второго секретаря посольства Брунея, Вашингтон, Джессике Сара (Jessica Sarra), директору департамента глобальных операций Международного центра по пропавшим без вести и эксплуатируемым детям (21 марта 2006 года) (в базе данных Международного центра по пропавшим без вести и эксплуатируемым детям).

[39] Статья 159(3) Уголовно-процессуального кодекса Болгарии, в сочетании со Статьей 159(1), объявляет вне закона, помимо прочего, "**распространяемые иными способами** работы, содержащие [детскую] порнографию" *Выделение добавлено авторами отчета.*

Страна	Специальное законодательство по детской порнографии	Дано определение "Детской порнографии"	Преступления, совершенные с использованием компьютера	Просто владение	Сообщения поставщиков услуг интернета (ISP)
Канада	✓	✓	✓	✓	✗ [40]
Кабо-Верде	✓	✗	✗	✗	✗
Центрально-Африканская Республика	✗	✗	✗	✗	✗
Чад	✗	✗	✗	✗	✗
Чили	✓	✓	✓	✗	✗

[40] Хотя в законах нет требования об обязательном сообщении, написанного специально для ISP, ISP в Канаде сотрудничают и тесно взаимодействуют с органами охраны правопорядка для упрощения сообщения о преступных материалах. Канадское уголовное законодательство использует очень широкое определение "детской порнографии", которое придает ее всеохватывающему набору преступлений дополнительных охват. Конкретные преступления по передаче, предоставлению и доступе были добавлены в 2002 году для учета возможностей интернета, и применяются к действиям ISP. Тем же законодательством Канада также ввела положение об "уведомлении и отключении" детской порнографии, обнаруженной в интернете. Наказания за преступления, связанные с детской порнографией, были ужесточены в 2005 году: установлены обязательные минимальные наказания; повышены максимальные наказания в виде суммарного заключения от 6 до 18 месяцев заключения; использование любой детской порнографии с намерением извлечения выгоды определено, как отягчающее обстоятельство при вынесении приговора; считая разоблачение и устрашение главными целями приговора в любом деле о жестоком обращении с ребенком; и считая жестокое обращение с любым ребенком отягчающим фактором при вынесении приговора. В дополнение к всесторонней защите, предусмотренной уголовным законодательством, Канада также имеет национальную общедоступную линию связи для сообщений о сексуальной эксплуатации ребенка в онлайновой среде (www.Cybertip.ca), которая выполняет сортировку этих сообщений для передачи их в органы охраны правопорядка. Кроме того, Cybertip.ca также поддерживает базу данных Канадского проекта Cleanfeed, который блокирует доступ к сайтам почти для 90% канадских абонентов, о которых известно, что они содержат детскую порнографию, но не подпадают под канадское уголовное право. Кроме того, в Канаде имеется национальная стратегия по защите детей от сексуальной эксплуатации в интернете, ключевым компонентом которой является Национальный координационный центр (Центр) по эксплуатации детей. Центр, который расположен при канадской конной полиции, координирует внутренние и внешние расследования сексуальной эксплуатации детей в он-лайне, обеспечивает обучение для канадских органов охраны правопорядка, и является центральным пунктом сортировки для сообщений, полученных по линии Cybertip.ca. Краткое содержание писем от Кэрол Моренси (Carole Morency), генерального консула Отдела Политики и уголовного законодательства Министерства юстиции Канады, Джессике Сара (Jessica Sarra), директору департамента глобальных операций Международного центра по пропавшим без вести и эксплуатируемым детям (24 июня 2008 года) (полное письмо находится в базе данных Международного центра по пропавшим без вести и эксплуатируемым детям).

Страна	Специальное законодательство по детской порнографии	Дано определение "Детской порнографии"	Преступления, совершенные с использованием компьютера	Просто владение	Сообщения поставщиков услуг интернета (ISP)
Китай[41]	✓[42]	✗	✓[43]	✗	✗
Колумбия	✓	✓	✓	✗	✓
Коморские Острова	✗	✗	✗	✗	✗
Конго	✗	✗	✗	✗	✗
Коста-Рика	✓	✓	✗	✓	✗
Кот-д'Ивуар	✗	✗	✗	✗	✗
Хорватия	✓	✗	✓	✓	✗

[41] Законодательство о детской порнографии в Гонконге отличается от законодательства Китая. Законодательство в Гонконге:
- определяет детскую порнографию;
- квалифицирует как преступление преступления, совершенные с использованием компьютера; и
- квалифицирует как преступление простое владение детской порнографией.

[42] Хотя в Китае нет специального законодательства о детской порнографии, в уголовном кодексе существует общий запрет на порнографические материалы. В 2004 году с целью обеспечить лучшую защиту несовершеннолетних Высший народный суд и Высший народный протекторат обнародовали "Интерпретацию некоторых проблем относительно выполнения законов о рассмотрении уголовных дел, касающихся производства, копирования, публикации, продажи, распространения порнографической электронной информации с использованием интернета, терминалов мобильной связи и радиостанций". Статья 6 этой Интерпретации прямо говорит, что "любой, кто распространяет, копирует, публикует или продает порнографическую электронную информацию, которая изображает сексуальные действия подростков до 18 лет, или предоставляет прямые ссылки на сервер интернета или веб-сайты, которые владеют, регулируют или используют для своих нужд электронную информацию, зная, что такая информация изображает сексуальные действия подростков до 18 лет, должен понести суровое наказание в соответствии со Статьей 363 Уголовного законодательства, регулирующей наказания за преступления по производству, копированию, публикации, продаже, распространению, или со Статьей 364 , регулирующей наказания за преступления по распространению порнографических материалов с тяжкими последствиями". Электронное письмо от Чен Фенг (Chen Feng) – сотрудника по связям с общественностью Посольство Народной Республики Китай, Вашингтон, Джессике Сара (Jessica Sarra), директору департамента глобальных операций Международного центра по пропавшим без вести и эксплуатируемым детям (17 марта 2006 года) (в базе данных Международного центра по пропавшим без вести и эксплуатируемым детям).

[43] Опубликованная в 2004 г. Интерпретация Высшего народного суда и высшего народного протектората относится к преступлениям, совершенным с использованием компьютера.

Страна	Специальное законодательство по детской порнографии	Дано определение "Детской порнографии"	Преступления, совершенные с использованием компьютера	Просто владение	Сообщения поставщиков услуг интернета (ISP)
Куба	✗	✗	✗	✗	✗
Кипр	✓	✓	✓	✓	✗
Чешская Республика	✓	✗	✓	✓	✗[44]
Демократическая Республика Конго	✗	✗	✗	✗	✗
Дания	✓	✓	✓[45]	✓	✗
Джибути	✗	✗	✗	✗	✗
Доминика	✗	✗	✗	✗	✗
Доминиканская Республика	✓	✓	✓	✓	✗
Эквадор	✓	✗	✗	✗	✗
Египет	✓	✗	✓	✓	✗

[44] Хотя в чешских законах нет требования об обязательном сообщении со стороны ISP, Чешский национальный план борьбы с коммерческой сексуальной эксплуатацией детей, опубликованный по адресу: http://www.mvcr.cz/prevence/priority/kszd/en_tab.html, называет Министерство транспорта и связи и Министерство внутренних дел национальными организациями, в обязанности которых входит определение предписанных законом обязательств для поставщиков услуг интернета, перечисленных в законе о связи (No. 151/2000) по сбору необходимых данных о незаконных веб-сайтах и передачи их в органы охраны правопорядка Чехии. Ожидаемым результатом этих мер является сохранность "доказательных фактов" против тех, кто распространяет в интернете детскую порнографию".

[45] Раздел 235 Датского Уголовного кодекса квалифицирует как преступление, помимо прочего, распространение и владение "другими …визуальными воспроизведениями" порнографических материалов, касающихся детей до 18 лет.

Страна	Специальное законодательство по детской порнографии	Дано определение "Детской порнографии"	Преступления, совершенные с использованием компьютера	Просто владение	Сообщения поставщиков услуг интернета (ISP)
Эль Сальвадор	✓	✗	✓	✓	✗
Экваториальная Гвинея	✗	✗	✗	✗	✗
Эритрея	✗	✗	✗	✗	✗
Эстония	✓	✗	✓[46]	✓	✗
Эфиопия	✗	✗	✗	✗	✗
Фиджи	✗	✗	✗	✗	✗
Финляндия	✓	✓	✓[47]	✓	✗
Франция	✓	✓	✓	✓	✓
Габон	✗	✗	✗	✗	✗
Гамбия	✓	✗	✗	✗	✗
Грузия	✓	✓	✗	✗	✗

[46] Статьи 177 и 178 Уголовно-процессуального кодекса Эстонии квалифицируют как преступление использование несовершеннолетних на "иных работах" или использование "любых других способов" производства, хранения, передачи, воспроизведения или предоставления доступа к детской порнографии.

[47] Глава 17, Раздел 18 Уголовного закона Финляндии квалифицирует как преступника "любое лицо, которое … другими способами распространяет порнографические изображения или видеозаписи, на которых изображены дети".

Страна	Специальное законодательство по детской порнографии	Дано определение "Детской порнографии"	Преступления, совершенные с использованием компьютера	Просто владение	Сообщения поставщиков услуг интернета (ISP)
Германия	✓	✓	✓	✓	✗[48]
Гана	✗	✗	✗	✗	✗
Греция	✓	✓	✓[49]	✓	✗
Гренада	✗	✗	✗	✗	✗
Гватемала	✓	✗	✗	✗	✗
Гвинея	✗	✗	✗	✗	✗
Гвинея-Бисау	✗	✗	✗	✗	✗
Гайана	✗	✗	✗	✗	✗
Гаити	✗	✗	✗	✗	✗
Гондурас	✓	✓	✓	✓	✗

[48] Хотя в законах нет явного требования к ISP обязательно сообщать в органы охраны правопорядка или другую компетентную организацию, в большинстве случаев ISP представляют отчеты в органы охраны правопорядка. Для ISP является уголовно наказуемым преступлением, если он знает о материалах с детской порнографией на своем веб-сайте и не удалит этот незаконный контент. При рассмотрении учитываются такие факторы, как возможно и разумно для ISP обнаруживать данные и удалять, или блокировать их, поскольку в Германии многие ISP предоставляют большие объемы для хранения данных с коммерческими целями. Электронное письмо от Клауса Германна (Klaus Hermann), Консула, сотрудника по связям с полицией, посольство Германии, Вашингтон, Джессике Сара (Jessica Sarra), директору департамента глобальных операций Международного центра по пропавшим без вести и эксплуатируемым детям (9 февраля 2006 года) (в базе данных Международного центра по пропавшим без вести и эксплуатируемым детям).

[49] Статья 348a Уголовно-процессуального кодекса Греции квалифицирует как преступления различные преступления, связанные с детской порнографией, включая владение, приобретение, пересылку и продажу детской порнографии "любым способом".

Страна	Специальное законодательство по детской порнографии	Дано определение "Детской порнографии"	Преступления, совершенные с использованием компьютера	Просто владение	Сообщения поставщиков услуг интернета (ISP)
Венгрия	✓	✓	✓[50]	✓	✗
Исландия	✓	✗	✓[51]	✓	✗
Индия	✓	✗	✓	✓	✗
Индонезия	✗	✗	✗	✗	✗
Иран	✗	✗	✗	✗	✗
Ирак	✗	✗	✗	✗	✗
Ирландия	✓	✓	✓	✓	✗
Израиль	✓	✓	✓	✓	✗
Италия	✓	✓	✓	✓	✗
Ямайка	✗	✗	✗	✗	✗
Япония	✓	✓	✓	✗	✗

[50] В соответствии с Разделом 195/A(3) Уголовного кодекса Венгрии, лицо, производящее, распространяющее или торгующее порнографическими изображениями несовершеннолетних в виде видеороликов, фильмов, фотографий или "при помощи любых других средств", либо помещающий такие изображения в открытом доступе для широкой общественности, совершает уголовное преступление. Более того, в соответствии с недавним решением Апелляционного суда Венгрии (Nr. BH 133/2005), понятия "любые другие средства" и "размещение в общем доступе для населения" включают в себя распространение через интернет. Письмо от Виктора Сжедеркений (Viktor Szederkényi), Заместителя руководителя службы, Посольство республики Венгрия, Вашингтон, Джессике Сара (Jessica Sarra), директору департамента глобальных операций Международного центра по пропавшим без вести и эксплуатируемым детям (6 февраля 2006 года) (в базе данных Международного центра по пропавшим без вести и эксплуатируемым детям).

[51] Статья 210 Уголовно-процессуального кодекса Исландии квалифицирует как преступление "владение фотографиями, фильмами или **сравнимыми** предметами, изображающими детей в сексуальной или порнографической манере". *Выделение добавлено авторами отчета.*

Страна	Специальное законодательство по детской порнографии	Дано определение "Детской порнографии"	Преступления, совершенные с использованием компьютера	Просто владение	Сообщения поставщиков услуг интернета (ISP)
Иордания	✗	✗	✗	✗	✗
Казахстан	✓	✗	✗	✗	✗
Кения	✗	✗	✗	✗	✗
Корея	✓	✓	✓	✗	✗
Кувейт	✗	✗	✗	✗	✗
Кыргызстан	✓	✗	✗	✗	✗
Лаос	✗	✗	✗	✗	✗
Латвия	✓	✗	✓[52]	✗	✗
Ливан	✗	✗	✗	✗	✗
Лесото	✗	✗	✗	✗	✗
Либерия	✗	✗	✗	✗	✗
Ливия	✗	✗	✗	✗	✗

[52] Статья 166(2) Уголовного законодательства Латвии квалифицирует как преступление "импорт, производство, публичную демонстрацию, рекламу, или иные **способы распространения** таких порнографических… материалов, как изображающие или относящиеся к сексуальной эксплуатации детей". *Выделение добавлено авторами отчета.*

Страна	Специальное законодательство по детской порнографии	Дано определение "Детской порнографии"	Преступления, совершенные с использованием компьютера	Просто владение	Сообщения поставщиков услуг интернета (ISP)
Лихтенштейн	✓	✗	✓	✓	✗[53]
Литва	✓	✗	✗	✓	✗
Люксембург	✓	✗	✓[54]	✓	✗
Македония	✓	✗	✓[55]	✗	✗
Мадагаскар	✓	✗	✓[56]	✗	✗
Малави	✗	✗	✗	✗	✗
Малайзия	✗	✗	✗	✗	✗
Мальдивские Острова	✗	✗	✗	✗	✗
Мали	✓	✗	✗	✗	✗
Мальта	✓	✗	✓	✓	✗

[53] Несмотря на то, что в Уголовно-процессуальном кодексе Лихтенштейна нет специального указания на сообщения поставщиков услуг интернета (ISP), в проекте нового закона о детях и молодежи предусмотрено требование об обязательном сообщении, которое будет относиться к "любому, узнавшему об опасности для благополучия ребенка или молодого человека". Электронное письмо от Клаудии Фритше (Claudia Fritsche), посла, Посольство Лихтенштейна, Вашингтон, Джессике Сара (Jessica Sarra), директору департамента глобальных операций Международного центра по пропавшим без вести и эксплуатируемым детям (7 февраля 2006 года) (в базе данных Международного центра по пропавшим без вести и эксплуатируемым детям).

[54] Статья 383 Уголовно-процессуального кодекса Люксембурга квалифицирует как преступление не только производство и владение с целью продажи, распространения или публичной демонстрации "рукописных, печатных, фотографических материалов, фильмов или **других объектов** порнографической природы", но так же совершение различных других преступлений, "любым способом" связанными с детской порнографией. *Выделение добавлено авторами отчета.*

[55] Статья 193(3) Уголовно-процессуального кодекса Македонии квалифицирует как преступление эксплуатацию "юных" при "производстве…других объектов с порнографическим контентом".

[56] Статья 346 Уголовно-процессуального кодекса Мадагаскара квалифицирует как преступление использование "любых средств" для распространения детской порнографии.

Страна	Специальное законодательство по детской порнографии	Дано определение "Детской порнографии"	Преступления, совершенные с использованием компьютера	Просто владение	Сообщения поставщиков услуг интернета (ISP)
Маршалловы Острова	✗	✗	✗	✗	✗
Мавритания	✗	✗	✗	✗	✗
Маврикий	✓	✗	✓	✗	✗
Мексика	✓	✓	✓	✗	✗
Молдавия	✓	✗	✗	✓	✗
Монако	✗	✗	✗	✗	✗
Монголия	✗	✗	✗	✗	✗
Черногория	✓	✗	✓[57]	✗	✗
Марокко	✓	✗	✗	✓	✗
Мозамбик	✗	✗	✗	✗	✗
Мьянма	✓	✗	✗	✗	✗
Намибия	✗	✗	✗	✗	✗
Науру	✗	✗	✗	✗	✗

[57] Статья 211(2) Уголовно-процессуального кодекса Черногории квалифицирует как преступление "эксплуатацию ребенка при производстве фотографий, аудио-визуальных или **других предметов** с порнографическим контентом". *Выделение добавлено авторами отчета.*

Страна	Специальное законодательство по детской порнографии	Дано определение "Детской порнографии"	Преступления, совершенные с использованием компьютера	Просто владение	Сообщения поставщиков услуг интернета (ISP)
Непал	✓	✗	✗[58]	✗	✗
Нидерланды	✓	✓	✓	✓	✗[59]
Нидерландские Антильские острова	✗[60]	✗	✗[61]	✗[62]	✗
Новая Зеландия	✓	✓	✓	✓	✗
Никарагуа	✗	✗	✗	✗	✗
Нигер	✗	✗	✗	✗	✗
Нигерия	✗	✗	✗	✗	✗
Норвегия	✓	✓	✓	✓	✗
Оман	✗	✗	✗	✗	✗
Пакистан	✗	✗	✗	✗	✗

[58] Несмотря на то, что Раздел 47 Указаний об электронных транзакциях 2004 года не относится специально к детской порнографии, он запрещает публикацию или демонстрацию на компьютерах, в интернете или в других электронных средствах информации материалов, которые запрещены законом к публикации или воспроизведению, потому что они противоречат общественной морали и порядочности.

[59] Несмотря на то, что нет законодательно установленных требований для ISP сообщать о подозрениях относительно детской порнографии в органы охраны правопорядка, ISP Нидерландов сразу же сообщают об обнаружении детской порнографии в органы охраны правопорядка, и ISP удаляют такой контент с соответствующих веб-сайтов. Далее, по запросу органов охраны правопорядка ISP просматривают свои логии на предмет подозрительных веб-сайтов. Электронные письма от Ричарда Гердлинга (Richard Gerding), канцлера по полицейским и юридическим вопросам, Королевское Посольство Нидерландов, Вашингтон, Джессике Сара (Jessica Sarra), директору департамента глобальных операций Международного центра по пропавшим без вести и эксплуатируемым детям (8) (в базе данных Международного центра по пропавшим без вести и эксплуатируемым детям).

[60] Несмотря на то, что специального законодательства по детской порнографии пока еще не существует, создан комитет по пересмотру существующего Уголовно-процессуального кодекса Нидерландских Антильских островов. Специальное законодательство по детской порнографии будет введено (Предлагаемая Статья 2.13.4). Электронное письмо от Ричарда Гердлинга (Richard Gerding), канцлера по полицейским и юридическим вопросам, Королевское Посольство Нидерландов, Вашингтон, Джессике Сара (Jessica Sarra), директору департамента глобальных операций Международного центра по пропавшим без вести и эксплуатируемым детям (22 февраля 2006 года) (в базе данных Международного центра по пропавшим без вести и эксплуатируемым детям).

[61] Предлагаемая Статья 2.13.4 квалифицирует как преступление преступления, совершенные с использованием компьютера.

[62] Предлагаемая Статья 2.13.4 квалифицирует как преступление простое владение.

Страна	Специальное законодательство по детской порнографии	Дано определение "Детской порнографии"	Преступления, совершенные с использованием компьютера	Просто владение	Сообщения поставщиков услуг интернета (ISP)
Панама	✓	✓	✓	✓	✗[63]
Папуа-Новая Гвинея	✓	✗	✗	✓	✗
Парагвай	✓	✗	✗	✓	✗
Перу	✓	✓	✓	✓	✗
Филиппины	✓	✗	✗	✗	✗
Польша	✓	✗	✗	✓	✗
Португалия	✓	✗	✓[64]	✓	✗
Катар	✓	✗	✓[65]	✗	✗
Румыния	✓	✓	✓	✓	✗

[63] Несмотря на то, что нет обязательных требований о сообщении, написанных специально для ISP, Статья 231-I Уголовно-процессуального кодекса Панамы устанавливает, что любой, кто знает об использовании несовершеннолетних в порнографии или сексуальных действиях, вне зависимости от того, получил ли человек эту информацию в результате выполнения своих обязанностей, работы, бизнеса, профессии или любыми другими средствами, и не сообщил об этом властям, он или она должны быть приговорены к тюремному заключению за это деяние. Если совершение преступления по детской порнографии или сексуальным действиям с детьми, о котором сообщено, невозможно доказать, то тот, кто сообщил будет освобожден от ответственности относительно его сообщения. Электронное письмо от Изабель Фернандес (Isabel Fernández), Посольство Панамы, Вашингтон, Джессике Сара (Jessica Sarra), директору департамента глобальных операций Международного центра по пропавшим без вести и эксплуатируемым детям (12, апреля 2006 года) (в базе данных Международного центра по пропавшим без вести и эксплуатируемым детям).

[64] Как можно видеть из Статьи 172 Уголовного закона Португалии, выражение "любыми средствами" позволяет прокурору рассматривать информационно-коммуникационные технологии как среду для совершения преступления по рассылке изображений, звуковых файлов или фильмов, на которых явно видны несовершеннолетние дети младше 14 лет, вовлеченные в сексуальные действия. Письмо от Педро Катарино (Pedro Catarino), Посла, Посольство Португалии, Вашингтон, Эмми Ален (Ernie Allen), Президенту и Генеральному директору Международного центра по пропавшим без вести и эксплуатируемым детям (24 февраля 2006 года) (в базе данных Международного центра по пропавшим без вести и эксплуатируемым детям).

[65] Статья 292 Уголовного кодекса Катара специально отмечает "книги, публикации, **другие печатные материалы**, изображения, фотографии, фильмы, символы или **другие предметы**". *Выделение добавлено авторами отчета.*

Страна	Специальное законодательство по детской порнографии	Дано определение "Детской порнографии"	Преступления, совершенные с использованием компьютера	Просто владение	Сообщения поставщиков услуг интернета (ISP)
Россия	✓	✗	✗	✗	✗
Руанда	✗	✗	✗	✗	✗
Сент-Киттс и Невис	✗	✗	✗	✗	✗
Сент-Люсия	✗	✗	✗	✗	✗
Сент-Винсент и Гренадины	✗	✗	✗	✗	✗
Сан-Марино	✓	✗	✓	✗	✗
Сан-Томе и Принсипи	✗	✗	✗	✗	✗
Саудовская Аравия	✗	✗	✗	✗	✗
Сенегал	✗	✗	✗	✗	✗
Сербия	✓	✗	✓[66]	✗	✗
Сейшельские Острова	✗	✗	✗	✗	✗

[66] Статья 111а Уголовно-процессуального кодекса Сербии квалифицирует как преступление создание "фотографии, фильма или **любого другого изображения**" несовершеннолетнего с целью создания объекта с порнографическим контентом. Статья 185 квалифицирует как преступление использование несовершеннолетнего с целью создания изображения, аудиовизуальных или **других объектов** с порнографическим контентом. *Выделение добавлено авторами отчета.*

Страна	Специальное законодательство по детской порнографии	Дано определение "Детской порнографии"	Преступления, совершенные с использованием компьютера	Просто владение	Сообщения поставщиков услуг интернета (ISP)
Сьерра-Леоне	✗	✗	✗	✗	✗
Сингапур	✗	✗	✗	✗	✗
Словацкая Республика	✓	✓	✓	✓	✗
Словения	✓	✓	✓[67]	✗	✗
Сомали	✗	✗	✗	✗	✗
Южная Африка	✓	✓	✓	✓	✓
Испания	✓	✗	✓[68]	✓	✗
Шри-Ланка	✓	✗	✗	✓	✗
Судан	✗	✗	✗	✗	✗
Суринам	✗	✗	✗	✗	✗
Свазиленд	✗	✗	✗	✗	✗

[67] Статья 187(2) Уголовно-процессуального кодекса Словении квалифицирует как преступление принуждение несовершеннолетнего "с целью создания изображения, аудиовизуальных или **других объектов** порнографического характера"; Статья 187(3) квалифицирует как преступление деяния любого, кто "создает, распространяет, продает, импортирует, экспортирует, … или поставляет [порнографические материалы с изображением несовершеннолетних] любым другим способом, или того, кто обладает такими материалами без намерения производить, распространять, продавать, импортировать, экспортировать или поставлять **любым другим способом**". *Выделение добавлено авторами отчета.*

[68] Статья 189(1)(a) Уголовно-процессуального кодекса Испании квалифицирует как преступление использование несовершеннолетнего с целью подготовки порнографического материала **любого вида**"; Статья 189(1)(b) квалифицирует как преступление производство, продажу, распространение, воспроизведение или содействие производству, продаже, распространению, или демонстрации "любого типа" детской порнографии при помощи "любых средств"; и Статья 189(7) повторяет ранее использованные фразы "любого типа" и "любых средств". *Выделение добавлено авторами отчета.*

Страна	Специальное законодательство по детской порнографии	Дано определение "Детской порнографии"	Преступления, совершенные с использованием компьютера	Просто владение	Сообщения поставщиков услуг интернета (ISP)
Швеция	✓	✗	✓[69]	✓	✗[70]
Швейцария	✓	✓	✓	✓	✗
Сирия	✗	✗	✗	✗	✗
Таджикистан	✓	✗	✗	✗	✗
Танзания	✓	✗	✗	✗	✗
Таиланд	✗	✗	✗	✗	✗
Тимор-Лешти	✗	✗	✗	✗	✗
Того	✗	✗	✗	✗	✗
Тонга	✓	✓	✓	✓	✗
Тринидад и Тобаго	✗	✗	✗	✗	✗

[69] Уголовное законодательство Швеции, в принципе, сформулировано так, что оно должно применяться вне зависимости от технических параметров. Детская порнография квалифицирует как преступление без каких-либо исключений, Глава 16, Раздел 10a, Уголовно-процессуального кодекса Швеции распространяет действие закона на преступления, совершенные с использованием компьютера. Письмо от Анетт Нильсон (Anette Nilsson), первого секретаря Посольства Швеции, Вашингтон, Джессике Сара (Jessica Sarra), директору департамента глобальных операций Международного центра по пропавшим без вести и эксплуатируемым детям (23 февраля 2006) (в базе данных Международного центра по пропавшим без вести и эксплуатируемым детям).

[70] В 1998 году Швеция приняла Закон об ответственности (1998:112) электронных досок объявлений (BBS), целью которого является предотвращение распространения детской порнографии, обязав поставщиков услуг BBS контролировать контент BBS. Поставщики услуг BBS также обязаны удалять либо иным способом предотвращать распространение сообщений с преступным контентом, включая сообщения с детской порнографией. Письмо от Анетт Нильсон (Anette Nilsson), первого секретаря Посольства Швеции, Вашингтон, Джессике Сара (Jessica Sarra), директору департамента глобальных операций Международного центра по пропавшим без вести и эксплуатируемым детям (23 февраля 2006) (в базе данных Международного центра по пропавшим без вести и эксплуатируемым детям).

Страна	Специальное законодательство по детской порнографии	Дано определение "Детской порнографии"	Преступления, совершенные с использованием компьютера	Просто владение	Сообщения поставщиков услуг интернета (ISP)
Тунис	✓	✗	✓[71]	✗	✗
Турция	✓	✗	✗	✓	✗
Туркменистан	✗	✗	✗	✗	✗
Уганда	✗	✗	✗	✗	✗
Украина	✓	✗	✓	✗	✗
Объединенные Арабские Эмираты	✗	✗	✗	✗	✗
Соединенное Королевство[72]	✓	✓	✓	✓	✗[73]
США	✓	✓	✓	✓	✓
Уругвай	✓	✗	✓[74]	✗	✗
Узбекистан	✗	✗	✗	✗	✗

[71] Статья 234 Уголовно-процессуального кодекса Туниса квалифицирует как преступление, помимо прочего, использование "любых видеозаписей или фотографий", на которых содержатся порнографические изображения детей.

[72] В данном Отчете Соединенное Королевство включает в себя Англию и Уэллс.

[73] В Соединенном Королевстве действует добровольная процедура "уведомления и отключения ", предусмотренная Фондом контроля интернета (IWF), независимой организацией отрасли, которой поручено полицией и правительством Соединенного Королевства контролировать, чтобы ISP "удаляли изображения детской порнографии", когда их уведомляет об этом IWF. Если они этого не сделают, то им может быть предъявлено обвинение. Письмо от Тони Лорд (Tony Lord), первого секретаря по вопросам юстиции и внутренним вопросам, Посольство Великобритании, Вашингтон, Ален (Ernie Allen), Президенту и Генеральному директору Международного центра по пропавшим без вести и эксплуатируемым детям (9 февраля 2006 года) (в базе данных Международного центра по пропавшим без вести и эксплуатируемым детям).

[74] Закон 17.815 Восточной Республики Уругвай квалифицирует как преступление определенные преступления, связанные с детской порнографией вне зависимости от того, как они совершены (т. е. Статья 1: "любыми способами производит или создает детскую порнографию "; Статья 2: " любыми способами содействует коммерциализации, распространению, воспроизведению, хранению или приобретению детской порнографии").

Страна	Специальное законодательство по детской порнографии	Дано определение "Детской порнографии"	Преступления, совершенные с использованием компьютера	Просто владение	Сообщения поставщиков услуг интернета (ISP)
Ватикан	✗[75]	✗	✗	✗	✗[76]
Венесуэла	✓	✓	✓	✗	✗
Вьетнам	✗	✗	✗	✗	✗
Йемен	✗	✗	✗	✗	✗
Замбия	✗	✗	✗	✗	✗
Зимбабве	✗	✗	✗	✗	✗

[75] В отсутствие специального законодательства по детской порнографии, по запросу Святого Престола такие дела могут быть переданы в итальянскую юридическую систему.

[76] "Святой Престол не имеет внешнего поставщика услуг интернета и системы навигации внутренних поставщиков имеют фильтры, которые закрывают не только доступ на любые сайты, связанные с детской порнографией, но также и с онлайновым распространением порнографических материалов. Учитывая, что веб-сайт Святого Престола является корпоративным, то на нем можно найти только те материалы, которые относятся к его работе". Письмо Архиепископа Пьетро Самби (Pietro Sambi), Апостольского нунция Апостольской Нунциатуры, Соединенные Штаты Америки, Эмми Ален (Ernie Allen), Президенту и Генеральному директору Международного центра по пропавшим без вести и эксплуатируемым детям (5 июня 2006 года) (в базе данных Международного центра по пропавшим без вести и эксплуатируемым детям).

Приложение 3

Программы для обеспечения безопасности ребенка

На рынке имеется множество пакетов программ и технических средств, которые помогают обнаружить нежелательный или ненужный контент и контакты, помогают ограничить время, в которое компьютер может получить доступ в интернет или ограничить приложения, которые могут запускаться на конкретном компьютере или устройстве. Некоторые операционные системы также содержат такие инструменты в качестве компонента стандартной поставки. Как правило, эти функции лежат в основе или поддерживают основные сообщения о безопасности, которые привычны для кампаний за безопасный интернет во всем мире. Программы безопасности такого типа широко используются в школах и общественных библиотеках и похожи на те программы, которые работодатели могут развернуть в своих внутренних сетях для ограничения неприемлемого или не связанного с работой использования интернета в рабочее время.

Эффективность программ для обеспечения безопасности ребенка может быть самой разной, и в некоторых странах прилагаются усилия по введению "печати одобрения", которая давала бы базовый уровень гарантии качества и которая помогала бы родителям, учителям, детям и молодым людям выбирать программы, которые наилучшим способом удовлетворяют их потребности и которые вероятно будут эффективно работать простым для понимания образом.

Всегда следует помнить, что каждое устройство рано или поздно сломается и каждая программа может работать неправильно. Поэтому родители, учителя, дети и молодые люди никогда не должны полностью перекладывать свою ответственность на программы обеспечения безопасности. Такие программы должны всегда рассматриваться как дополнение к обучению и программам повышения осведомленности, предназначенным для гарантии того, что ребенок или молодой человек знает, как избежать онлайновых угроз, или знает, как их решать, если они возникают.

Примеры существующих в настоящее время пакетов программ обеспечения безопасности ребенка включают в себя:

Бесплатные продукты

1 K9 Web Protection (http://www.k9webprotection.com/)

2 SafeFamilies (http://www.safefamilies.org/download.php)

3 File Sharing Sentinel (http://www.akidthaine.com/)

4 B-Gone (http://support.it-mate.co.uk/?mode=Products&p= bgone)

5 Последние версии Windows и Mac OS также включают в себя инструменты, которые могут использоваться без дополнительной платы

Коммерческие продукты

- Net Nanny Parental Controls
- Safe Eyes
- CYBERsitter
- WiseChoice.net
- CyberPatrol
- MaxProtect
- FilterPak
- Netmop
- imView
- McAfee Parental Controls
- Norton Parental Controls
- Child Safe
- ContentProtect Security Appliance
- http://www.cybersentinel.co.uk/

Более подробный список как коммерческих, так и бесплатных продуктов размещен по адресу www.getnetwise.org.

Приложение 4

Разработка национальной стратегии

Интернет сделал возможным целый спектр способов жестокого обращения с детьми и молодыми людьми, например, при помощи веб-камер и чатов, которые были попросту нереальными до его появления как продукта массового потребления. Интернет также играет отдельную роль в расширении масштабов, в которых материалы САМ становятся доступными во всех уголках мира. По этим причинам при снятии озабоченности относительно онлайновой безопасности для детей и молодых людей, директивные органы могут пожелать уделить особое внимание некоторым или всем из следующих положений:

1 Объявить вне закона "груминг" или другие формы дистанционного заманивания несовершеннолетних к неприемлемым сексуальные контактам или сексуальным действиям.

2 Объявить вне закона владение, производство и распространение материалов САМ, вне зависимости от наличия намерения их распространять.

3 Предпринять дополнительные меры по прекращению или уменьшению трафика передачи материалов САМ, например, создав национальную горячую линию и внедряя меры, которые будут блокировать доступ к веб-сайтам и новостным группам Usenet, о которых известно, что они содержат или рекламируют наличие материалов САМ.

4 Обеспечить наличие национальных процессов, которые гарантируют, что все обнаруженные в стране материалы САМ будут направлены в централизованный национальный ресурс.

5 Разработать стратегии контроля спроса на материалы САМ, в частности, со стороны тех, кто уже был наказан за совершение таких преступлений. Важно повышать осведомленность в том, что это преступление не относится к преступлениям без жертв: дети используются для создания материала, который просматривается путем просмотра и скачивания на международном уровне материалов САМ, какое-либо лицо вносит свой непосредственный вклад в жестокое обращение с изображенным там ребенком, а также поощряет использование большего числа детей для создания большего числа изображений.

6 Повысить осведомленность в том, что дети никогда не согласятся с тем, что их сексуально используют, для производства материалов САМ или любым другим способом. Призывайте людей, использующих материалы САМ, к поискам помощи, и в то же время, сообщая им, что они будут нести уголовную ответственность за незаконные действия, в которые они вовлечены.

7 Обеспечить такое положение дел, при котором стратегии охраны правопорядка и предотвращения преступлений, а также школьные и социальные программы содержали бы разделы по кибербезопасности и разделы о

рисках, создаваемых поведением интернет-хищника в онлайновом режиме, а также советы, соответствующие возрасту.

8 Рассмотреть другие стратегии контроля спроса на материалы CAM. Например, в некоторых странах ведется регистр осужденных сексуальных преступников. Суды выписывают юридические предписания, запрещающих таким преступникам пользоваться интернетом либо совсем, либо использовать те области интернета, которые часто посещают дети и молодые люди. Проблема с этими предписаниями заключается в том, как обеспечить их выполнение. Однако в некоторых странах рассматривается вопрос объединения списка известных сексуальных преступников в список блокировки, не дающий им возможности посещать или регистрироваться на определенных веб-сайтах, например, веб-сайтах, о которых известно, что их посещает множество детей и молодых людей. Конечно, если преступник зарегистрируется на веб-сайте, используя другое имя или фальшивый логин, эффективность таких мер значительно снизится, объявив такое поведение незаконным, можно создать еще одно сдерживающее средство.

9 Обеспечить жертвам соответствующую долгосрочную поддержку. В тех случаях, когда дети или молодые люди стали онлайновыми жертвами, например, если в интернете появилось их незаконное изображение, они вполне естественно будут беспокоиться о том, кто его может увидеть, и какие последствия это будет иметь для них. Это может заставлять ребенка или молодого человека чувствовать себя уязвимым для запугивания или дальнейшей сексуальной эксплуатации и жестокого обращения. В этом контексте важно, чтобы были доступны службы поддержки для детей и молодых людей, которые оказались в такой ситуации. Такая поддержка может требоваться на долгосрочной основе.

10 Обеспечить создание и широкое продвижение механизма, который обеспечивает легкопонятные и быстродействующие средства для сообщения о незаконном контенте либо о незаконном или подозрительном поведении в онлайновом режиме, например, системы, аналогичной той, которая была создана Виртуальной глобальной целевой группой http://www.virtualglobaltaskforce.com. Следует поощрять и использование системы INTERPOL i24/7.

11 Обеспечить такое положение дел, при котором достаточное количество сотрудников органов охраны правопорядка прошли соответствующее обучение по расследованиям преступлений, совершенных в интернете или с использованием компьютеров, а также имеют доступ к соответствующим средствам криминалистики, позволяющим им выделять и интерпретировать соответствующие цифровые данные.

12 Инвестировать в обучение сотрудников органов охраны правопорядка, прокуратуры и юстиции методам, используемым онлайновыми преступниками для совершения таких преступлений.

Инвестиции также потребуются на приобретение и обслуживание оборудования, необходимого для получения и интерпретации криминалистических доказательств из цифровых устройств. В дополнение будет важно создать двустороннее и многостороннее сотрудничество и обмен информацией с соответствующими организациями охраны правопорядка и следственными органами в других странах.

Фотографии предоставлены 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, 2009 г.

При поддержке:

Child Helpline International

unicri
advancing security, serving justice, building peace

International Centre
FOR MISSING & EXPLOITED CHILDREN

CHIS