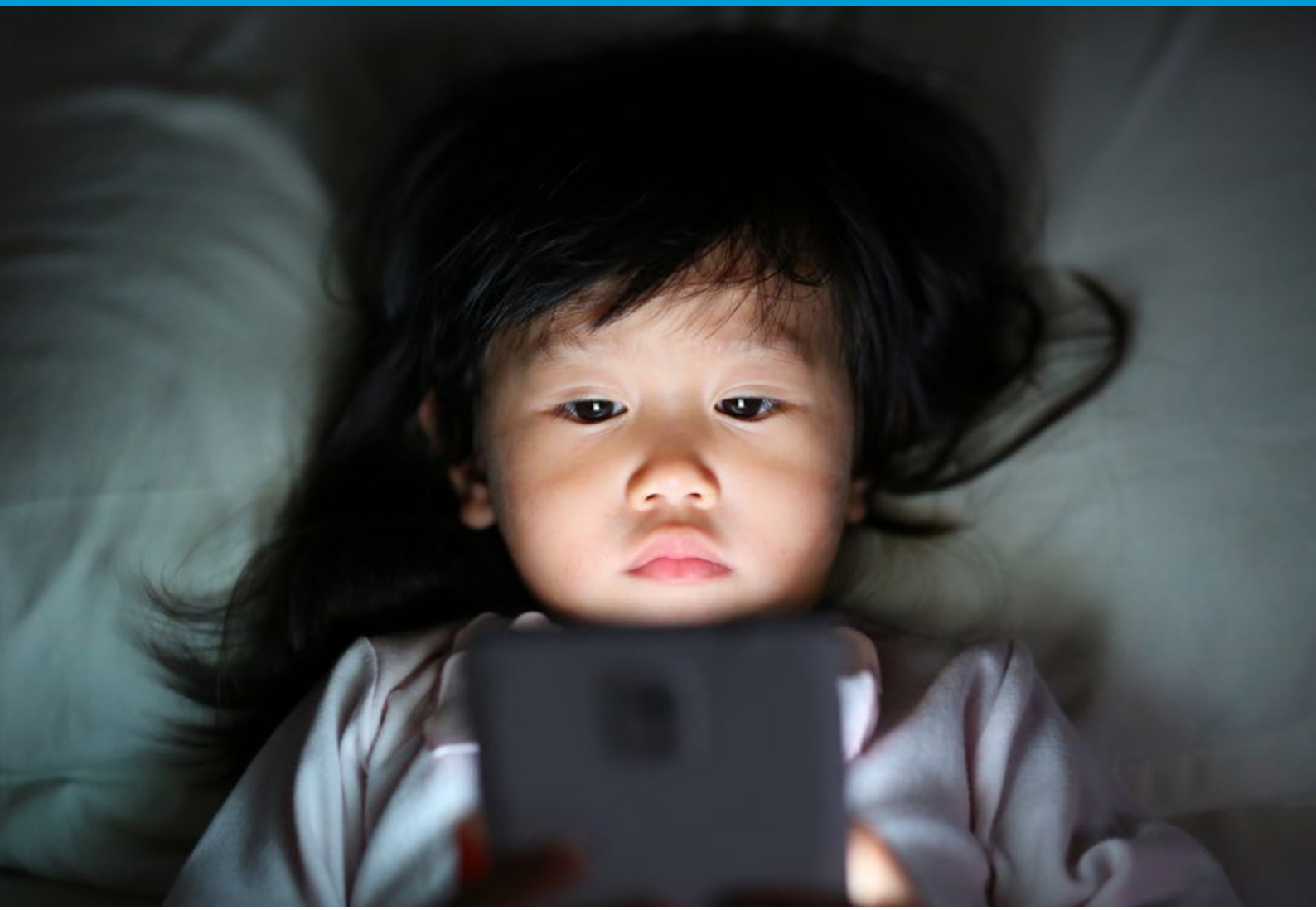
ITUПубликации

Международный союз электросвязи
Сектор развития

Руководящие указания для директивных органов по защите ребенка в онлайновой среде

2020



Руководящие указания для директивных органов по защите ребенка в онлайновой среде

2020 год

Выражение признательности

Настоящие Руководящие указания разработаны Международным союзом электросвязи (МСЭ) и рабочей группой авторов из ведущих учреждений, работающих в отрасли информационно-коммуникационных технологий (ИКТ) и занимающихся проблемами защиты ребенка (в онлайновой среде), в том числе из следующих организаций:

ECPAT International, сеть Global Kids Online, Глобальное партнерство по прекращению насилия в отношении детей, проект HABLATAM, Сеть центров безопасного интернета Insafe, Интерпол, Международный центр по пропавшим без вести и эксплуатируемым детям (ICMEC), Международный союз инвалидов, Международный союз электросвязи (МСЭ), Фонд наблюдения за интернетом (IWF), Лондонская школа экономики, Канцелярия Специального представителя Генерального секретаря по вопросу о насилии в отношении детей и Специальный докладчик по вопросу о торговле детьми и сексуальной эксплуатации детей, Privately SA, RNW Media, Центр безопасного интернета Соединенного Королевства, Глобальный альянс WePROTECT (WPGA) и Всемирный фонд детства в США.

Рабочая группа осуществляла свою деятельность под председательством Дэвида Райта (Центр безопасного интернета Соединенного Королевства/SWGfL) и при координирующей роли Фанни Ротино (МСЭ).

Данные Руководящие указания не смогли бы состояться без затраченного авторами времени, присущего им энтузиазма и самоотверженности. Неоценимый вклад внесли также COFACE-Families Europe, Совет Европы, Комиссариат по электронной безопасности Австралии, Европейская комиссия, Группа e-Worldwide Group (e-WWG), ОЭСР, Молодежь и социальные сети / Центр Беркмана Клейна по вопросам интернета и общества Гарвардского университета, а также правительства отдельных стран и заинтересованные отраслевые организации, объединенные общей целью – сделать интернет лучшим и более безопасным местом для детей и молодежи.

Ниже перечислены партнеры, которым МСЭ выражает признательность за то, что они посвятили свое время этой работе и поделились своими знаниями (перечисление приводится в алфавитном порядке по названию организаций):

- Мартин Шмальцрид (COFACE-Families Europe)
- Ливия Стойка (Совет Европы)
- Джон Карр (ECPAT International)
- Джулия Фосси и Элла Серри (Комиссариат по вопросам электронной безопасности)
- Мануэла Марта (Европейская комиссия)
- Сальма Аббаси (e-WWG)
- Эми Крокер и Серена Томмасино (Глобальное партнерство по прекращению насилия в отношении детей)
- Лионель Бросси (HABLATAM)
- Сандра Марченко (ICMEC)
- Карл Хопвуд (Insafe)[1]
- Люси Ричардсон (Международный союз инвалидов)
- Мэтью Домпьер (Интерпол)
- Фанни Ротино (МСЭ)
- Тесс Лейлэнд (IWF)
- Соня Ливингстон (Лондонская школа экономики и Global Kids Online)

[1] По поручению Европейской комиссии в рамках фонда "Соединяющаяся Европа" (CEF) организация "European Schoolnet" запустила платформу "Better Internet for Kids" ("Более безопасный интернет для детей") и осуществляет координацию Европейской сети Центров безопасного Интернета (Insafe). Дополнительная информация размещена по адресу: www.betterinternetforkids.eu.

- Элеттра Ронки (ОЭСР)
- Манус де Барра (Канцелярия Специального представителя Генерального секретаря по вопросу о насилии в отношении детей)
- Дипак Тевари (Privately SA)
- Павитра Рам (RNW Media)
- Мод де Бер-Букиккио (Специальный докладчик по вопросу о торговле детьми и сексуальной эксплуатации детей)
- Дэвид Райт (Центр безопасного интернета Соединенного Королевства/SWGfL)
- Иэн Дреннан и Сюзанна Ричмонд (Глобальный альянс WePROTECT)
- Лина Фернандес и д-р Джоанна Рубинштейн (Всемирный фонд детства в США)
- Сандра Кортези (Молодежь и социальные сети)

ISBN

978-92-61-30084-5 (бумажная версия)

978-92-61-30414-0 (электронная версия)

978-92-61-30074-6 (версия EPUB)

978-92-61-30424-9 (версия Mobi)

Просьба подумать об окружающей среде, прежде чем печатать этот отчет

Предисловие

В современном мире, который характеризуется проникновением интернета практически во все сферы жизни, обеспечение защиты молодых пользователей в онлайновой среде становится все более насущной задачей для каждой страны.

Свой первый комплект Руководящих указаний по защите ребенка в онлайновой среде МСЭ разработал еще в 2009 году. С того времени интернет претерпел разительные изменения. Он превратился в бесконечно богатый источник игр и знаний для детей, однако в то же время он стал для них гораздо более опасным местом для занятий без присмотра.

В настоящее время дети сталкиваются с многочисленными рисками: от проблем защиты конфиденциальности до контента с элементами насилия и другого неподобающего контента, интернет-мошенничества, а также угроз в виде груминга в онлайновой среде, сексуальных злоупотреблений и сексуальной эксплуатации. Количество угроз возрастает, при этом преступники все чаще действуют одновременно в нескольких юрисдикциях, что сказывается на эффективности мер реагирования и возмещения ущерба, принимаемых в рамках отдельных государств.

Кроме того, в период глобальной пандемии COVID-19 произошло резкое увеличение количества детей, впервые присоединившихся к онлайновому миру, чтобы получать помощь в обучении и поддерживать социальное взаимодействие. Введение ограничений в связи с вирусом привело не только к тому, что многие дети младшего возраста начали общаться в интернете гораздо раньше, чем планировали их родители, но и к тому, что многие родители, вынужденные выполнять свои должностные обязанности, оказались не в состоянии присматривать за детьми, что в свою очередь поставило последних перед лицом опасности получить доступ к неприемлемому контенту или стать мишенью преступников, занимающихся производством материалов, связанных с сексуальными злоупотреблениями в отношении детей.

Сегодня больше, чем когда-либо прежде, для обеспечения безопасности детей в онлайновой среде необходимо международное сотрудничество и координация усилий, которые требуют активного участия и поддержки со стороны широкого круга заинтересованных лиц: как представителей отрасли, включая частные платформы, поставщиков услуг и операторов сетей, так и правительственных структур и гражданского общества.

Осознавая это, в 2018 году Государства – Члены МСЭ попросили предоставить нечто большее, нежели очередное обновление Руководящих указаний по СОР, которое до этого проводилось на периодической основе. Таким образом, эти новые пересмотренные руководящие указания были переосмыслены, переписаны и полностью переработаны от начала и до конца, чтобы отразить фундаментальные изменения, произошедшие в цифровой среде, в которой находятся дети.

Помимо того, что в этом новом издании нашли отражение новые тенденции в цифровых технологиях и платформах, в нем восполнен один серьезный пробел: положение, в котором находятся дети-инвалиды, которым онлайновый мир предлагает жизненно важное средство коммуникации, обеспечивая им возможность полноценного участия в социальной жизни. В этом документе также учтены особые потребности детей из числа мигрантов и других уязвимых групп.

Мы надеемся, что настоящие руководящие указания будут служить прочным фундаментом для разработки директивными органами всеохватных национальных стратегий с участием многих заинтересованных сторон, включая открытые консультации и диалог с детьми, для принятия более адресных и эффективных мер.

Работая над составлением новых руководящих указаний, МСЭ и его партнеры стремились создать максимально практичную, гибкую и адаптируемую платформу, основанную на международных стандартах и общих целях, включая положения Конвенции о правах ребенка и Цели ООН в области устойчивого развития. У меня вызывает чувство гордости тот факт, что эти пересмотренные руководящие указания были разработаны в рамках глобальных совместных усилий в истинном духе МСЭ, его роли как глобального организатора и координатора, и при активном участии международных экспертов из широкого многостороннего сообщества.

Я также рада представить вам наш новый талисман COP – Санго, доброжелательный, смелый и бесстрашный персонаж, полностью разработанный группой детей в рамках новой международной программы МСЭ по повышению осведомленности молодежи.

В эпоху, когда все больше и больше молодых людей приобщаются к онлайновым технологиям, настоящие Руководящие указания по COP приобретают особую важность. Директивные органы, представители отрасли, родители, педагоги, а также сами дети – все играют исключительно важную роль. Как всегда, я благодарна вам за поддержку и рассчитываю на дальнейшее тесное сотрудничество по этому важному вопросу.

Дорин Богдан-Мартин
Директор Бюро развития электросвязи

Вступление

Тридцать лет назад правительства практически всех государств взяли на себя обязательство соблюдать, защищать и поощрять права детей. Конвенция ООН о правах ребенка (КПР) является наиболее широко ратифицированным международным договором по правам человека за всю историю. Несмотря на значительный прогресс, достигнутый за эти три десятилетия, наряду с сохраняющимися серьезными вызовами появляются новые источники рисков для безопасности детей.

В 2015 году все государства вновь заявили о своей приверженности правам ребенка, приняв повестку дня на период до 2030 года и 17 всеобщих целей в области устойчивого развития (ЦУР). Например, цель 16.2 заключается в том, чтобы к 2030 году положить конец надругательствам, эксплуатации и всем формам насилия и пыток в отношении детей. В целом же защита детей является связующей темой для 11 из 17 ЦУР. ЮНИСЕФ ставит детей в центр повестки дня на период до 2030 года, как показано на Рисунке 1.

Рисунок 1: Дети, ИКТ и ЦУР

В Повестке дня в области устойчивого развития на период до 2030 года признается, что ИКТ могут играть ключевую роль в достижении ЦУР. Распространение информационно-коммуникационных технологий (ИКТ) и глобальное взаимное подключение сетей открывают возможности для ускорения человеческого прогресса, преодоления цифрового разрыва и формирования обществ, основанных на знаниях. Также определены конкретные задачи, связанные с использованием ИКТ для достижения устойчивого развития в сфере образования (цель 4), гендерного равенства (цель 5), инфраструктуры (цель 9 – всеобщий и недорогой доступ к интернету) и цели 17 – партнерство и средства осуществления[1]. ИКТ способны полностью трансформировать экономику, поскольку являются движущей силой в достижении каждой из 17 ЦУР. ИКТ уже демонстрируют свою эффективность, расширяя права и возможности миллиардов людей во всем мире за счет обеспечения доступа к образовательным ресурсам и здравоохранению, а также предоставления некоторых услуг, в частности таких, как электронное правительство и социальные сети.

Таким образом, стремительное распространение информационно-коммуникационных технологий дало детям и молодым людям беспрецедентные возможности для общения, подключения, обмена, обучения, доступа к информации и выражения своего мнения по вопросам, которые касаются их собственной жизни и жизни их сообществ.

Однако расширение и упрощение доступа к интернету и технологиям подвижной связи также сопряжено с серьезными вызовами для безопасности и благополучия детей как в онлайновой среде, так и в реальной жизни.

[1] UNDP, Sustainable Development Goals | UNDP, undp.org, дата обращения: 29 января 2020 года, https://www.undp.org/content/undp/en/home/sustainable-development-goals.html; Хоулинь Чжао, "Почему ИКТ имеют решающее значение для достижения ЦУР", МСЭ, ITU News Magazines, 48, дата обращения: 29 января 2020 года, https://www.itu.int/en/itunews/Documents/2017/2017-03/2017_ITUNews03-ru.pdf.

Чтобы снизить риски, которые несет в себе цифровой мир, и одновременно сделать так, чтобы больше детей и молодых людей могли пользоваться его благами, правительства, представители гражданского общества, местные сообщества, международные организации и отраслевые предприятия должны объединить свои усилия ради общей цели. Особенно важную роль в выполнении общемировой задачи по обеспечению защиты детей в онлайновой среде играют директивные органы.

Для преодоления вызовов, связанных с быстрым развитием ИКТ и защитой детей от последствий этого явления, в ноябре 2008 года Международным союзом электросвязи (МСЭ) была запущена многосторонняя международная инициатива "Защита ребенка в онлайновой среде" (COP). Эта инициатива призвана объединить партнеров из всех секторов мирового сообщества в интересах создания безопасных и расширяющих возможности условий в онлайновой среде для детей во всем мире.

Кроме того, участники Полномочной конференции Международного союза электросвязи 2018 года в Дубае вновь подтвердили важность инициативы COP, признав ее в качестве эффективной платформы для повышения осведомленности, обмена передовым опытом, а также оказания содействия и поддержки Государствам-Членам, особенно развивающимся странам, в разработке и реализации дорожных карт в области COP. Также была признана важность обеспечения защиты детей в онлайновой среде в рамках Конвенции ООН о правах ребенка и других международных договоров по правам человека путем поощрения сотрудничества между всеми заинтересованными сторонами, занимающимися вопросами защиты ребенка в онлайновой среде.

Участники Конференции признали важность Повестки дня в области устойчивого развития на период до 2030 года, которая затрагивает различные аспекты защиты ребенка в онлайновой среде в рамках Целей устойчивого развития (ЦУР), в том числе ЦУР 1, 3, 4, 5, 9, 10 и 16; также была принята во внимание Резолюция 175 (Пересм. Дубай, 2018 г.) о доступе к электросвязи/информационно-коммуникационным технологиям (ИКТ) для лиц с ограниченными возможностями и особыми потребностями и Резолюция 67 (Пересм. Буэнос-Айрес, 2017 г.) Всемирной конференции по развитию электросвязи (ВКРЭ) о роли Сектора развития электросвязи МСЭ (МСЭ-D) в защите ребенка в онлайновой среде.

В конце 2019 года Комиссия МСЭ/ЮНЕСКО по широкополосной связи в интересах устойчивого развития выпустила отчет "Безопасность ребенка в онлайновой среде", в котором содержатся применимые на практике рекомендации в отношении того, как сделать интернет безопаснее для детей.

В 2009 году МСЭ выпустил первый набор руководящих указаний по защите ребенка в онлайновой среде в рамках инициативы COP. За последнее десятилетие Руководящие указания COP были переведены на многие языки и используются во многих странах мира в качестве справочного ресурса при разработке дорожных карт и национальных стратегий по защите ребенка в онлайновой среде. Они служат подспорьем для государственных органов, организаций гражданского общества, учреждений по уходу за детьми, отраслевых организаций и многих других заинтересованных сторон в их усилиях по защите ребенка в онлайновой среде.

В частности, эти руководящие указания использовались при составлении, разработке и осуществлении национальных стратегий по защите ребенка в онлайновой среде во многих Государствах-Членах, таких как Камерун, Габон, Гамбия, Гана, Кения, Сьерра-Леоне, Уганда и Замбия в Африканском регионе; Бахрейн и Оман в Арабском регионе; Бруней, Камбоджа, Кирибати, Индонезия, Малайзия, Мьянма и Вануату в Азиатско-Тихоокеанском регионе; Босния, Грузия, Молдова, Черногория, Польша и Украина в Европейском регионе.

Кроме того, эти руководящие указания легли в основу региональных мероприятий, таких как Региональная конференция по защите ребенка в онлайновой среде (ACOP) "Расширение прав и возможностей будущих цифровых граждан", которая прошла в Кампале (Уганда, 2014 г.), и Региональная конференция АСЕАН по защите ребенка в онлайновой среде, состоявшаяся в Бангкоке (Таиланд, 2020 г.)

Согласно Резолюции 179 (Пересм. Дубай, 2018 г.), МСЭ было поручено обновить четыре комплекта руководящих указаний в сотрудничестве с партнерами по инициативе COP и заинтересованными сторонами с учетом развития технологий в отрасли электросвязи, в том числе руководящие указания в отношении детей-инвалидов и детей с особыми потребностями.

По итогам этого процесса данные руководящие указания были в значительной степени обновлены и пересмотрены экспертами и соответствующими заинтересованными сторонами, которые подготовили обширный комплекс рекомендаций по обеспечению защиты детей в цифровом мире. Они являются продуктом совместных многосторонних усилий и подготовлены на основе знаний, опыта и экспертной оценки многих организаций и специалистов во области защиты детей в онлайновой среде со всего

мира. Эти руководящие указания призваны послужить основой для создания безопасного и надежного кибермира для будущих поколений. Предполагается, что эти указания станут программой, которая может быть адаптирована и использована в соответствии с национальными или местными традициями и законами. Кроме того, эти руководящие указания посвящены вопросам, которые затрагивают всех детей и молодых людей младше 18 лет, с учетом различий в потребностях каждой возрастной группы. Они также направлены на удовлетворение нужд детей, живущих в различных условиях, детей-инвалидов и детей с особыми потребностями. Настоящие руководящие указания также расширяют охват мер по защите детей в онлайновой среде, учитывая все риски, угрозы и вредное воздействие, которым могут подвергаться дети в онлайновой среде, в соотношении с положительными изменениями, которые цифровой мир может привнести в их жизнь.

Ожидается, что эти руководящие указания не только позволят создать более открытое информационное общество, но и помогут Государствам – Членам МСЭ выполнить свои обязательства по защите и реализации прав детей, как предусмотрено в Конвенции ООН о правах ребенка[2], которая была принята Генеральной Ассамблеей ООН в резолюции 44/25 от 20 ноября 1989 года, и итоговом документе Всемирной встречи на высшем уровне по вопросам информационного общества[3](ВВУИО).

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

---

[2] UNICEF, "Convention on the Rights of the Child", uncief.org, дата обращения: 29 января 2000 года, https://www.unicef.org/child-rights-convention.

[3] ВВУИО проводилась в два этапа: в Женеве (10–12 декабря 2003 г.) и в Тунисе (16–18 ноября 2005 г.). По итогам ВВУИО было принято твердое 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".

Содержание

Список таблиц, рисунков и вставок

Таблицы

Рисунки

Вставки

1 Обзор документа

1.1 Цель

Национальные правительства обязаны обеспечивать защиту детей как в реальном, так и в виртуальном мире. Необходимо понимать, что сегодня, когда новые технологии так прочно интегрированы в жизнь столь большого числа детей и молодых людей в ряде важных областей, более не имеет смысла пытаться сохранять четкое разделение между событиями реального мира и онлайновыми событиями. Они все больше пересекаются и зависят друг от друга.

Директивные органы[1] и все другие соответствующие заинтересованные стороны играют чрезвычайно важную роль. В условиях стремительного развития технологий многие традиционные методы разработки политики оказываются непригодными. Для того чтобы обеспечить защиту детей в онлайновой среде, директивным органам необходимо разработать адаптивную и всеохватную нормативно-правовую базу, которая будет выполнять свое предназначение в контексте быстро меняющейся цифровой среды.

Настоящие руководящие указания разработаны с тем, чтобы предоставить директивным органам Государств – Членов МСЭ удобную в использовании и гибкую основу для понимания и выполнения ими своих правовых обязательств по обеспечению защиты детей в реальном, то есть физическом, и виртуальном мирах.

С этой целью в настоящих руководящих указаниях освещается ряд важных для директивных органов вопросов:

1) Что такое защита детей в онлайновой среде?

2) Почему директивные органы должны беспокоиться о защите детей в онлайновой среде?

3) Какова ситуация в моей стране с точки зрения законодательства, социально-политических условий и развития?

4) Как директивным органам следует начинать рассмотрение и определение эффективной и последовательной политики по защите детей в онлайновой среде в их стране?

При этом данные руководящие указания разработаны на основе существующих моделей, механизмов и ресурсов, с тем чтобы рассмотреть конкретные примеры и получить представление о передовой практике, применяемой в различных странах мира.

1.2 Сфера применения

Сфера применения мер по защите детей в онлайновой среде распространяется на любой вред, который может быть причинен ребенку в онлайновой среде, включая широкий спектр факторов, угрожающих безопасности и благополучию детей. Это комплексная проблема, к решению которой следует подходить с разных сторон, в том числе с точки зрения законодательства, управления, образования, политики и общества.

Кроме того, защита ребенка в онлайновой среде должна основываться на понимании как общих, так и конкретных для каждой страны рисков, угроз и вредного воздействия, которым подвергаются дети в цифровой среде. Это требует четкого определения понятий и установления ясных параметров для вмешательства, в которых учитываются и разграничиваются действия, являющиеся преступлением, и действия, которые не являются противозаконными, но тем не менее представляют угрозу для благополучия ребенка.

С этой целью в руководящих указаниях представлен обзор существующих угроз и вредного воздействия, которым подвергаются дети в цифровой среде. Вместе с тем в условиях быстрого развития технологий и появления новых сопутствующих угроз и источников вредного воздействия традиционные сроки и методы разработки политики оказываются неэффективными. В цифровую эпоху директивным органам необходимо создавать такие правовые и политические рамки, которые будут достаточно адаптивными и открытыми для всех, чтобы решать существующие проблемы и по мере возможности предвидеть будущие вызовы. Для этого необходимо сотрудничество со всеми заинтересованными сторонами, включая отрасль

[1] Термин "директивные органы" в настоящем документе используется для обозначения всех заинтересованных сторон, ответственных за разработку и осуществление политики, включая правительственные структуры.

ИКТ, научное сообщество, гражданское общество, общественность и самих детей. Этот процесс может быть подкреплен рассмотрением общих принципов, касающихся защиты ребенка в онлайновой среде.

1.3 Общие принципы

Одиннадцать всеобъемлющих принципов, которые приводятся ниже, в своей совокупности послужат подспорьем в разработке перспективной целостной национальной стратегии по защите ребенка в онлайновой среде.

Порядок, в котором представлены эти принципы, продиктован не степенью их важности, а скорее логикой повествования.

Национальная стратегия по защите детей в онлайновой среде должна:

1) основываться на целостном видении, в котором учитывается роль правительства, отрасли и общества;
2) формулироваться исходя из всеобъемлющего понимания и анализа цифровой среды в целом и корректироваться с учетом национальных условий и приоритетов конкретной страны;
3) согласовываться с основополагающими правами детей, как это закреплено в Конвенции ООН о правах ребенка, а также других ключевых международных конвенциях и нормах, и гарантировать соблюдение этих прав;
4) соответствовать существующим аналогичным или схожим внутренним законам и стратегиям, включая законы о недопущении жестокого обращения с детьми и стратегии по защите детей, и гарантировать их соблюдение;
5) гарантировать соблюдение гражданских прав и свобод детей, которыми нельзя пренебрегать ради обеспечения защиты;
6) разрабатываться при активном участии всех соответствующих заинтересованных сторон, включая детей, с учетом их потребностей и обязанностей, а также принимая во внимание нужды меньшинств и маргинализированных групп;
7) разрабатываться таким образом, чтобы соответствовать государственным программам более общего характера, направленным на достижение экономического и социального процветания, и обеспечивать максимальный вклад ИКТ в достижение устойчивого развития и социальной интеграции;
8) использовать наиболее адекватные инструменты политики для достижения поставленных целей с учетом специфических условий соответствующей страны;
9) осуществляться на самом высоком уровне в правительстве, которое будет отвечать за распределение соответствующих ролей и обязанностей, а также предоставление необходимых человеческих и финансовых ресурсов;
10) способствовать созданию такой цифровой среды для детей, родителей/опекунов и заинтересованных сторон, которой они смогут доверять;
11) направлять усилия заинтересованных сторон в целях расширения прав и возможностей детей, а также обучения детей цифровой грамотности, для того чтобы они могли защитить себя в онлайновой среде.

1.4 Использование настоящих руководящих указаний

В настоящих руководящих указаниях рассматриваются актуальные исследования, существующие модели и материалы, а также даются четкие рекомендации по разработке национальных стратегий по защите ребенка в онлайновой среде.

- В разделе 2 представлена вводная информация о защите детей в онлайновой среде и приводятся данные последних исследований, в том числе по аспектам, касающимся новых появляющихся технологий, основных угроз и вредного воздействия, которым подвергаются дети.
- В разделе 3 освещаются вопросы, касающиеся подготовки национальной стратегии в области защиты ребенка в онлайновой среде, включая соответствующие заинтересованные стороны, существующие примеры реагирования на угрозы и вредное воздействие в онлайновой среде, а также преимущества принятия национальной стратегии.

- В разделе 4 приводятся рекомендации в отношении соответствующих механизмов и порядка осуществления.
- В разделе 5 определен перечень ключевых аспектов, которые необходимо учесть при разработке национальной стратегии по ребенка детей в онлайновой среде.
- В разделе 6 представлены полезные справочные материалы.

2 Введение

В 2019 году интернетом пользовалось больше половины населения мира. Самая многочисленная группа пользователей – это люди моложе 44 лет, при этом отмечается одинаковая активность среди пользователей в возрасте от 16 до 24 лет и от 35 до 44 лет. Интернетом пользуется каждый третий ребенок (0–18 лет) во всем мире[2]. В развивающихся странах пользователями интернета являются преимущественно дети и молодые люди[3], и, согласно прогнозам, в течение следующих пяти лет их число увеличится более чем в два раза. Новые поколения пользуются интернетом с самого детства, причем большинство людей подключается к сети с помощью технологий подвижной связи, особенно в странах глобального Юга[4].

Несмотря на то, что доступ к интернету имеет основополагающее значение для осуществления прав детей, по-прежнему наблюдаются серьезные региональные, национальные, гендерные и иные диспропорции в получении доступа, которые ограничивают возможности девочек, детей-инвалидов, детей из числа меньшинств и других уязвимых групп. Что касается цифрового гендерного разрыва, то, как показывают исследования, во всех регионах мира, за исключением Соединенных Штатов Америки, серди пользователей интернета насчитывается значительно больше мужчин, чем женщин. Во многих странах девочки не имеют равных с мальчиками возможностей в плане доступа к интернету, а в тех случаях, когда они имеют равный доступ, их контролируют и ограничивают в использовании интернета намного больше, чем мальчиков, и они могут подвергаться рискам при попытках получить доступ к интернету[5]. Очевидно, что детям и молодым людям, не обладающим достаточными цифровыми навыками или говорящим на языках меньшинств, непросто найти нужный им контент в интернете и что дети, живущие в сельской местности, обладают менее развитыми цифровыми навыками, проводят больше времени в интернете (особенно играя в игры) и получают меньше помощи и контроля со стороны родителей[6].

Тем не менее невозможно говорить о рисках и угрозах без понимания того, насколько огромны преимущества и возможности, которые дают нам цифровые технологии. Интернет и цифровые технологии меняют наш образ жизни и открывают множество новых возможностей для общения, игр, прослушивания музыки и участия в разнообразных культурных, образовательных мероприятиях, мероприятиях по развитию навыков. Интернет служит средством получения необходимого доступа к услугам в области здравоохранения и образования, а также к информации по темам, которые имеют важное значение для молодых людей, но могут рассматриваться как табу в обществе, к которому они принадлежат.

Поскольку дети и молодые люди нередко находятся в авангарде применения и освоения новых возможностей, предоставляемых интернетом, они сталкиваются с различными явлениями, угрожающими их безопасности и благополучию; общество должно осознавать эту проблему и бороться с ней. Очень важно открыто обсуждать существующие риски, которым подвергаются дети и молодые люди в онлайновой среде. Такое обсуждение дает возможность научить детей и молодых людей распознавать

---

2 OECD, "New Technologies and 21st Century Children: Recent Trends and Outcomes", OECD Education Working Paper № 179 (Directorate for Education and Skills, OECD), дата обращения: 27 января 2020 года, https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=EDU/WKP%282018%2915&docLanguage=En.

3 Ofcom, "Children and Parents: Media Use and Attitudes Report 2018" (Ofcom), дата обращения: 17 января 2020 года, https://www.ofcom.org.uk/__data/assets/pdf_file/0024/134907/children-and-parents-media-use-and-attitudes-2018.pdf.

4 МСЭ, Отчет "Измерение информационного общества", дата обращения: 16 января 2020 года, https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ICTOI-2018-SUM-PDF-R.pdf.

5 "Young Adolescents and Digital Media: Uses, Risks and Opportunities in Low-and Middle-Income Countries", GAGE, дата обращения: 29 января 2020 года, https://www.gage.odi.org/publication/digital-media-risks-opportunities/.

6 Livingstone, S., Kardefelt Winther, D., and Hussein, M. (2019). *Global Kids Online Comparative Report, Innocenti Research Report*. UNICEF Office of Research – Innocenti, Florence, https://www.unicef-irc.org/publications/1059-global-kids-online-comparative-report.html. Это может иметь неожиданные последствия: так, исследование, проведенное HABLATAM в пяти странах Латинской Америки, показало, что в уязвимых сообществах дети могут использовать платформы для знакомств, видеоигры и социальные сети для перевода денег в незаконных целях. Conectados al Sur network, "Hablatam", Hablatam Project 2020, дата обращения: 6 февраля 2020 года, https://hablatam.net/.

риски, предотвращать или преодолевать вредное воздействие, в случае если они ему подверглись, а также использовать преимущества и возможности, которые может дать им интернет.

Во многих странах мира молодые люди хорошо осведомлены о некоторых рисках, с которыми они могут столкнуться в онлайновой среде[7, 8]. Например, как показывают исследования, большинство детей и молодых людей способны отличить кибертравлю от шуток или поддразнивания в интернете. Они понимают, что кибертравля носит публичный характер и направлена на причинение вреда, однако поиск баланса между возможностями и рисками, существующими для ребенка в онлайновой среде, по-прежнему остается сложной задачей[9].

Государства – Члены МСЭ продолжают уделять первостепенное внимание защите детей и молодых людей в онлайновой среде; при этом необходимо соблюдать надлежащий баланс между решением этой задачи и усилиями по расширению возможностей детей и молодых людей в онлайновой среде[10] и обеспечивать защиту детей и молодых людей таким образом, чтобы не ограничивать их доступ или доступ более широких групп населения к информации, а также возможность пользоваться правом на свободу слова, выражения мнений и ассоциации.

Существует очевидная необходимость в целенаправленной поддержке и выработке нестандартных решений для противодействия рискам, с которыми сталкиваются дети и молодые люди, в том числе из-за цифрового разрыва между детьми и взрослыми, который ограничивает возможность родителей, учителей и опекунов давать детям необходимые наставления. В то же время дети и молодые люди вырастают и становятся взрослыми людьми, родителями и активными членами общества, что дает им уникальную потенциальную возможность сократить этот цифровой разрыв.

В связи с этим укрепление доверия к интернету должно иметь первостепенное значение и занимать центральное место в государственной политике. Правительства и общество должны вести работу с детьми и молодыми людьми, чтобы понимать их точку зрения и инициировать подлинно общественные дебаты о рисках и возможностях. Оказание детям и молодым людям содействия в управлении онлайновыми рисками может быть эффективным, однако правительства также должны обеспечивать работу компетентных служб поддержки для тех, кому причиняется вред в онлайновой среде, а также информировать детей о том, как они могут обратиться в эти службы.

Некоторые страны делают все возможное, чтобы выделять необходимые ресурсы для решения проблемы цифровой грамотности и обеспечения безопасности детей в онлайновой среде. Однако сами дети говорят о том, что важную роль в разработке решений для поддержания их безопасности в онлайновой среде играют родители, учителя, технологические компании и правительства. Государства – Члены МСЭ также отмечают, что такие меры, как активизация обмена знаниями и координация усилий в целях обеспечения защиты большего числа детей в онлайновой среде, пользуются значительной поддержкой[9].

Детям и молодым людям приходится ориентироваться во все более сложных условиях цифровой среды, а внедрение искусственного интеллекта для машинного обучения, аналитика больших данных, роботизация, интернет вещей, виртуальная и дополненная реальность полностью изменят опыт взаимодействия детей с медийной средой. В связи с этим необходимы инвестиции и разработка политики для поддержки детей, родителей и сообществ как в настоящем, так и в будущем.

2.1 Что такое защита ребенка в онлайновой среде?

Благодаря онлайновым технологиям дети и молодые люди получают огромные возможности для общения, приобретения новых навыков, творчества и участия в создании лучшего общества. Однако эти технологии также могут создавать новые риски, связанные с конфиденциальностью, незаконным контентом, домогательствами, кибертравлей, злоупотреблением личной информацией или грумингом в сексуальных целях и даже сексуальными злоупотреблениями в отношении детей.

---

7 С 2016 года МСЭ проводит консультации в рамках СОР при участии детей и взрослых, представляющих соответствующие заинтересованные стороны, по актуальным вопросам, таким как кибертравля, цифровая грамотность и активность детей в онлайновой среде.

8 ITU, Youth Consultation, https://www.itu.int/en/council/cwg-cop/Pages/meetings.aspx.

9 UNICEF, "Global Kids Online Comparative Report (2019)".

10 ITU, "Celebrating 10 Years of Child Online Protection", ITU News, February 6, 2018, https://news.itu.int/celebrating-10-years-child-online-protection/.

Настоящие руководящие указания предлагают целостный подход к реагированию на все потенциальные угрозы и вредное воздействие, которым могут подвергаться дети и молодые люди в процессе овладения цифровой грамотностью. В них признается, что все соответствующие заинтересованные стороны играют важную роль в обеспечении устойчивости детей и молодых людей к воздействию цифровой среды, их благополучия и защиты при одновременном использовании ими возможностей, которые предоставляет интернет.

Защита детей и молодых людей является общей ответственностью, поэтому все соответствующие заинтересованные стороны должны внести свой вклад в достижение устойчивого будущего для всех. Для этого директивные органы, представители отрасли, родители, опекуны, педагоги и другие заинтересованные стороны должны способствовать тому, чтобы дети и молодые люди могли реализовывать свой потенциал – как в онлайновой среде, так и в реальной жизни.

Понятие защиты детей в онлайновой среде не имеет универсально закрепленного определения, однако оно предполагает целостный подход к созданию безопасных, рассчитанных на соответствующий возраст, открытых и основанных на широком участии цифровых пространств для детей и молодых людей при обеспечении:

- реагирования, поддержки и самопомощи при наличии угрозы;
- предотвращения вредного воздействия;
- динамичного равновесия между защитой и предоставлением детям возможности быть цифровыми гражданами;
- осуществления прав и обязанностей как детей, так и общества.

Кроме того, в условиях стремительного развития технологий и общества, а также с учетом безграничного характера интернета, для эффективной защиты детей в онлайновой среде необходим гибкий и адаптивный подход. В настоящих руководящих указаниях подробно рассматриваются основные риски, с которыми сталкиваются дети и молодые люди в онлайновой среде, включая вредоносный и незаконный контент, домогательства, кибертравлю, злоупотребление личной информацией или груминг в сексуальных целях, сексуальные злоупотребления в отношении детей и их сексуальную эксплуатацию, однако по мере развития технических инноваций будут возникать новые вызовы, которые, как всегда, будут различаться в зависимости от региона. При этом с новыми вызовами лучше всего бороться совместными усилиями в рамках всего мирового сообщества, поскольку эти вызовы будут требовать выработки новых решений.

2.2 Дети в цифровом мире

Интернет преобразил наш образ жизни. Он стал неотъемлемой составляющей жизни детей и молодых людей, сделав невозможным восприятие физической и цифровой реальностей в отрыве друг от друга. Сегодня дети и молодежь составляют треть от общего числа пользователей интернета; по оценкам ЮНИСЕФ, 71% молодых людей уже имеют доступ к интернету.

Распространение доступа к интернету значительно расширило возможности людей. Онлайновый мир позволяет детям и молодым людям преодолевать ограничения, связанные с неблагоприятным положением или инвалидностью, предоставляет новые форматы развлечений, образования, участия и выстраивания отношений. Сегодня цифровые платформы используются для различных видов деятельности и часто имеют мультимедийный характер.

Наличие доступа к этим технологиям, умение пользоваться ими и ориентироваться в этой среде имеют большое значение для развития молодых людей, поэтому эти технологии используются ими с раннего возраста. Директивные органы должны понимать, что зачастую дети и молодые люди начинают пользоваться различными платформами и услугами до того, как достигают установленного возрастного минимума, поэтому обучение должно начинаться с малых лет.

Дети и молодые люди хотят участвовать в обсуждении этой проблемы; будучи представителями цифрового поколения, они обладают ценным опытом и знаниями, которыми они могут поделиться. Директивные органы и специалисты-практики должны находиться в непрерывном диалоге с детьми и молодыми людьми по вопросам онлайновой среды в целях поддержки соблюдения их прав.

Доступ к интернету

В 2019 году интернетом пользовалось больше половины населения мира (53,6%): количество пользователей составляло приблизительно 4,1 миллиарда. Каждый третий пользователь интернета во всем мире – это ребенок моложе 18 лет[1]. В некоторых странах с низким уровнем дохода это соотношение составляет один к двум, а в странах с более высоким уровнем дохода – примерно один к пяти. По данным ЮНИСЕФ, доступ к интернету есть уже у 71% молодых людей во всем мире[2]. Таким образом, присутствие детей и молодых людей в интернете становится значительным, постоянным и неизменным[3]. Интернет используется в различных социальных, экономических и политических целях, превращается в семейный, потребительский продукт или услугу и становится неотъемлемым атрибутом жизни семей, детей и молодых людей.

Данные за 2017 год свидетельствуют о том, что в различных регионах доступ детей и молодых людей к интернету в значительной степени зависит от уровня дохода. Как правило, в странах с низким уровнем дохода насчитывается меньше детей, пользующихся интернетом, нежели в странах с высоким уровнем дохода.

В большинстве стран дети и молодые люди проводят в интернете больше времени в выходные дни, нежели в будни, причем больше всего времени в сети проводят подростки (15–17 лет) – в среднем от 2,5 до 5,3 часов, в зависимости от страны.

Использование интернета

Для выхода в интернет дети и молодые люди чаще всего используют мобильный телефон, на втором и третьем месте – настольный компьютер и ноутбук соответственно. Дети и молодые люди проводят в интернете в среднем около двух часов в день в течение недели и примерно в два раза больше времени в выходные дни. Некоторые остаются подключенными непрерывно. Однако немало и тех, кто до сих пор не имеет возможности выхода в интернет из дома.

На практике большинство детей и молодых людей, пользующихся интернетом, подключаются с помощью нескольких устройств: дети и молодые люди, которые подключаются к интернету по меньшей мере раз в неделю, могут использовать до трех различных устройств. Дети старшего возраста, а также дети в более богатых странах, как правило, используют больше устройств, причем во всех обследованных странах мальчики используют большее количество устройств, чем девочки.

Самый распространенный вид активности как среди девочек, так и среди мальчиков – это просмотр видеороликов. Более чем три четверти детей и молодых людей, пользующихся интернетом, говорят, что смотрят видео в интернете по меньшей мере раз в неделю вместе с другими членами семьи либо самостоятельно. Многих детей и молодых людей можно отнести к категории социально активных пользователей, поскольку они зарегистрированы сразу на нескольких платформах, таких как Facebook, Twitter, TikTok и Instagram.

Дети и молодые люди также используют интернет для участия в политике и ведут блоги для того, чтобы выражать свое мнение.

---

1 Livingstone, S., Carr, J., and Byrne, J. (2015) *One in three: The task for global internet governance in addressing children's rights*. Global Commission on Internet Governance: Paper Series. London: CIGI and Chatham House, https://www.cigionline.org/publications/one-three-internet-governance-and-childrens-rights.

2 Broadband Commission, "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online (2019)", *Broadband Commission for Sustainable Development,* October 2019, 84, https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf.

3 Livingstone, Carr, and Byrne, "One in Three: Internet Governance and Children's Rights".

Общий уровень участия в онлайновых играх варьируется в зависимости от страны и примерно соответствует степени доступности интернета для детей и молодых людей, при этом 10–30% детей и молодых людей, пользующихся интернетом, каждую неделю занимаются творческой деятельностью в онлайновом режиме.

Что касается образования, то многие дети и молодые люди всех возрастов пользуются интернетом каждую неделю, чтобы сделать домашнее задание, наверстать упущенное после пропуска занятий или найти информацию о здоровье. Дети старшего возраста, как представляется, проявляют больший интерес к поиску информации, чем дети помладше.

2.3 Влияние технологий на цифровой опыт детей

Интернет и цифровые технологии могут быть источником как возможностей, так и рисков для детей и молодых людей. Например, когда дети используют социальные сети, перед ними открываются многочисленные возможности для исследований, обучения, общения и развития основных навыков. В частности, социальные сети воспринимаются детьми как платформы, позволяющие им раскрывать собственную идентичность в безопасной среде. Обладание необходимыми навыками и знаниями о том, как разрешать проблемы, связанные с конфиденциальностью и репутацией, имеет большое значение для молодых людей.

"Я знаю, что все опубликованное нами в интернете остается там навсегда и может повлиять на нашу жизнь в будущем" (мальчик, 14 лет, Чили).

Тем не менее, как было установлено в процессе консультаций, большинство детей используют социальные сети до достижения минимально допустимого возраста, который составляет 13 лет[11], а службы проверки возраста, как правило, слаборазвиты или отсутствуют, поэтому риски, которым подвергаются дети, могут возрастать. Несмотря на то, что дети стремятся овладевать цифровыми навыками и быть добросовестными цифровыми гражданами, заботясь о неприкосновенности своей частной жизни, они склонны задумываться об этой проблеме в привязке к своим друзьям и знакомым: их больше беспокоит, что могут увидеть их друзья, нежели незнакомые люди и третьи лица. Все это, в совокупности с присущим детям любопытством и их большей подверженностью рискам, может сделать их более уязвимыми к грумингу, эксплуатации, травле или другим видам вредоносного контента либо контакта.

Широкая популярность обмена фотографиями и видео с помощью мобильных приложений, в частности использование детьми платформ потокового контента, также вызывает беспокойство по поводу неприкосновенности их частной жизни и возможных рисков. Некоторые дети делают фотографии сексуального характера с собственным участием, участием своих друзей, братьев или сестер и делятся ими в интернете. Для некоторых, особенно для детей старшего возраста, это может быть естественным проявлением сексуальности и поиском сексуальной идентичности, однако в других случаях, в частности это касается детей младшего возраста, речь идет о принуждении со стороны взрослого или другого ребенка. В любом случае подобный контент является незаконным во многих странах, он может стать причиной того, что ребенок подвернется преследованию, или может быть использован для дальнейшей эксплуатации ребенка.

Аналогичным образом, онлайновые игры позволяют детям реализовывать свои основополагающие права, в том числе право играть, устанавливать контакты, проводить время с друзьями, заводить новых друзей и развивать важные навыки. В большинстве случаев это может быть положительным опытом. Однако появляется все больше свидетельств, указывающих на то, что дети, использующие онлайновые игровые платформы без присмотра и без поддержки со стороны ответственного взрослого, также могут подвергаться рискам, таким как игровые расстройства, финансовые махинации, сбор и монетизация личных данных детей, кибертравля, агрессивные высказывания, насилие и неприемлемые контакты или контент[12], а также груминг с использованием реальных фотографий и видео либо картинок и видео, созданных компьютером или относящихся к виртуальной реальности, где изображаются или выставляются как норма сексуальные злоупотребления в отношении детей или их сексуальная эксплуатация.

[11] Conectados al Sur network, "Hablatam"; UNICEF, "Global Kids Online Comparative Report (2019)".
[12] UNICEF, "Global Kids Online Comparative Report (2019)" (UNICEF, 2019).

Кроме того, развитие технологий привело к появлению интернета вещей, который предполагает подключение все большего числа разнообразных устройств друг к другу, их взаимодействие и объединение в сети с помощью интернета. К таким предметам относятся игрушки, радионяни и устройства, работающие на основе искусственного интеллекта, что может создавать риски с точки зрения неприкосновенности частной жизни и нежелательных контактов.

2.4 Основные угрозы, которым подвергаются дети в онлайновой среде

Взрослые и дети подвергаются различным рискам и угрозам в онлайновой среде. Однако дети являются намного более уязвимой группой населения. Более того, некоторые категории детей находятся в особо уязвимом положении, например дети-инвалиды[13] или дети в процессе транзита. Директивные органы должны делать все необходимое, чтобы все дети могли развиваться и обучаться в безопасной цифровой среде. Мысль о том, что дети уязвимы и их следует защищать от всех форм эксплуатации, определена в Конвенции ООН о правах ребенка.

В некоторых областях цифровая среда открывает перед детьми огромные возможности, которые одновременно могут усугублять риски, способные причинить ребенку серьезный вред и подорвать его благополучие. Существуют опасения как в отношении детей, так и в отношении взрослых, что интернет, к примеру, может использоваться для вмешательства в частную жизнь, распространения дезинформации или, что еще хуже, доступа к порнографии.

В этом отношении важно проводить различие между рисками и вредным воздействием, которым подвергаются дети. Не все действия, которые по некоторым признакам могут расцениваться как риск, являются опасными, и не все риски обязательно наносят вред детям – например секстинг, который может использоваться молодыми людьми для раскрытия своей сексуальности и получения опыта отношений, что далеко не всегда причиняет вред.

Рисунок 2: Классификация угроз, которым подвергаются дети в онлайновой среде[14]

	Контент Ребенок как потребитель (массового производства)	Контакт Ребенок как участник (действия, инициированные взрослым)	Поведение Ребенок как активное действующее лицо (нарушитель/жертва)
Агрессивного характера	Жестокость/сцены насилия	Домогательства, преследование	Травля, враждебное поведение сверстников
Сексуального характера	Порнографические материалы	Груминг, сексуальные злоупотребления при встрече с незнакомцами	Сексуальные домогательства, секстинг
Ценностного характера	Расистский/ разжигающий ненависть контент	Идеологическое убеждение	Потенциально вредный контент, создаваемый пользователем
Коммерческого характера	Реклама, скрытый маркетинг	Использование персональных данных, в том числе ненадлежащее	Азартные игры, нарушение авторских прав

Источник: исследовательская сеть ЕС "Дети в онлайновой среде" (Ливингстон, Хаддон, Герциг и Олафссон (2011 г.)).

С наступлением цифровой эпохи появились новые вызовы, связанные с защитой детей. Дети должны иметь возможность чувствовать себя защищенными в онлайновой среде и пользоваться многочисленными благами, которые она предоставляет.

Директивные органы должны обеспечивать принятие необходимого законодательства, предоставление гарантий и разработку инструментов, для того чтобы дети могли развиваться и обучаться в безопасных

[13] Lundy et al., "TWO CLICKS FORWARD AND ONE CLICK BACK", Report on children with disabilities in the digital environment (Council of Europe, October 2019), https://rm.coe.int/two-clicks-forward-and-one-click-back-report-on-children-with-disabili/168098bd0f.

[14] Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011). *Risks and safety on the internet: The perspective of European children. Full findings*. LSE, London: EU Kids Online, http://eprints.lse.ac.uk/33731/.

условиях. Крайне важно, чтобы дети имели все необходимые навыки для определения угроз и полностью осознавали последствия и своего поведения в онлайновой среде.

В интернете дети могут столкнуться с многочисленными угрозами, исходящими от организаций, взрослых и сверстников.

Контент и манипуляция

- Столкнувшись с неприемлемым или даже преступным контентом, дети могут впадать в такие крайности, как причинение вреда самим себе, разрушительное и жестокое поведение. Воздействие такого контента может привести к радикализации детей, а также развитию у них интереса к расистским или дискриминационным идеям. Известно, что многие дети не соблюдают возрастные ограничения, установленные на веб-сайтах.
- Получение детьми неточной или неполной информации не позволяет им сформировать полноценное представление об окружающем мире. Тенденция к персонализации контента в зависимости от поведения пользователя может приводить к образованию "информационного пузыря", который не дает детям возможности развиваться и потреблять разнообразный контент.
- Воздействие контента, подвергнутого алгоритмической фильтрации с целью манипуляции, может оказать серьезное воздействие на развитие ребенка, его взгляды, ценности и привычки. Изоляция детей в "эхо-камере" или "информационном пузыре" ограничивает их доступ ко всему многообразию взглядов и идей.

Контакты со взрослыми или сверстниками

Дети могут сталкиваться с широким спектром угроз, вступая в контакт со взрослыми или сверстниками.

- Травля в интернете может иметь более широкие масштабы и распространяться быстрее, чем в офлайновой среде. Травля может осуществляться в любое время – днем или ночью, нарушая границы "пространства", прежде считавшегося безопасным, и может носить анонимный характер.
- Дети, которые становятся жертвами в реальной жизни, скорее всего будут подвергаться виктимизации в онлайновой среде. Таким образом, дети-инвалиды подвержены рискам в большей степени, поскольку, как показывают исследования, такие дети чаще становятся жертвами различного рода посягательств и особенно часто подвергаются сексуальной виктимизации. Виктимизация может включать в себя травлю, домогательства, изоляцию и дискриминацию на почве имеющейся или предполагаемой инвалидности ребенка или аспектов, связанных с его инвалидностью, таких как особенности поведения или речи, оборудование или услуги, которыми он пользуется.
- Диффамация и нанесения ущерба репутации: изображения и видео могут редактироваться и распространяться среди миллиардов людей. Неоправданно жестокие комментарии могут в течение многих лет оставаться доступными для просмотра.
- Дети могут подвергаться преследованию, грумингу и надругательствам в интернете со стороны обидчиков, которые могут находиться как поблизости, так и в другом конце мира и которые часто выдают себя за тех, кем они не являются. Такое воздействие может проявляться в различных формах, включая радикализацию и принуждение детей к тому, чтобы они сами отправляли контент сексуального характера со своим участием.
- Совершение покупок в результате давления, обмана или принуждения с разрешения плательщика или без него.
- В связи с нежелательной рекламой возникают вопросы, касающиеся согласия и продажи данных.

Поведение ребенка, которое может иметь последствия

- Травля в онлайновой среде может быть особенно неприятной или разрушительной, так как она распространяется в более широких масштабах, с большей степенью публичности, а контент, распространяемый с помощью электронных средств, может в любой момент вновь попасть в фокус внимания, в результате чего человеку, ставшему жертвой травли, может быть непросто забыть об инциденте; такой контент может содержать дискредитирующие визуальные изображения или оскорбительные слова; он доступен 24 часа в сутки; травля при помощи электронных средств связи может происходить 24 часа в сутки 7 дней в неделю, вторгаясь в частную жизнь жертвы даже там, где они должны чувствовать себя в безопасности, например дома; персональная информация

может быть искажена, фотографии изменены и затем переданы другим людям. Более того, травля может осуществляться анонимно. Раскрытие персональных данных может привести к причинению физического вреда, включая встречи в реальной жизни после знакомства в интернете, когда существует опасность физического насилия и/или сексуальных злоупотреблений.

- Несоблюдение собственных прав или прав других людей в процессе плагиата и загрузки в интернет контента без разрешения, в частности создание и размещение в интернете фотографий неподобающего содержания без разрешения.
- Нарушение авторских прав других людей, например, путем скачивания из интернета музыки, фильмов или ТВ программ, за которые следовало бы заплатить, поскольку это может причинить вред жертве кражи.
- Маниакальное или чрезмерное использование интернета и/или онлайновых игр в ущерб социальным мероприятиям и/или занятиям на свежем воздухе, важным для здоровья, укрепления доверия, социального развития и общего благополучия.
- Попытки причинения вреда, домогательства или травли в отношении кого-либо, в том числе когда злоумышленник выдает себя за другого человека, часто за другого ребенка.
- Среди подростков становится все более распространенным такое явление, как "секстинг" (отправка изображений или сообщений сексуального характера с помощью мобильных телефонов). Как правило, люди отправляют такие изображения и сообщения партнерам, с которыми они находятся в отношениях, либо потенциальным партнерам, однако иногда они оказываются доступными для более широкой аудитории. Маловероятно, что подростки в полной мере осознают последствия подобного поведения и потенциальные риски, которые оно может повлечь за собой.

2.5 Основные источники вреда для детей в онлайновой среде

В предыдущем разделе речь идет об угрозах, с которыми дети могут столкнуться онлайн. В этом разделе освещается вред, который может быть результатом этих угроз.

Источники вреда

Согласно исследованиям ЮНИСЕФ об использовании интернета, к рискам и источникам вреда относятся следующие категории:

- Причинение себе вреда:
  - контент, относящийся к суициду;
  - дискриминация.
- Воздействие неподходящих материалов:
  - воздействие экстремистского/насильственного контента;
  - скрытый маркетинг;
  - онлайновые азартные игры.
- Около 20 процентов детей, опрошенных по данной теме, сказали, что за прошедший год видели веб-сайты или дискуссии в сети о том, как люди причиняют себе физический вред или боль.
- Радикализация:
  - идеологическая обработка;
  - агрессивные высказывания.

– Дети с большей вероятностью сообщали о том, что были расстроены агрессивными высказываниями или контентом сексуального характера в сети, что с ними обращались ненадлежащим образом в онлайновой среде или в реальном мире, или тем, что они встретились с кем-то лицом к лицу, с кем сначала познакомились в сети.

– Сексуальные злоупотребления и сексуальная эксплуатация:

  • собственноручно созданный контент;

  • груминг в сексуальных целях;

  • материалы, связанные с сексуальными злоупотреблениями в отношении детей (CSAM);

  • торговля людьми;

  • сексуальная эксплуатация детей в путешествиях и туризме.

Проведенное в 2017 году исследование положения детей в Дании, Венгрии и Соединенном Королевстве показало, что у 6 процентов детей были откровенные фотографии, которые передавались без их разрешения.

В 2019 году Фонд наблюдения за интернетом (IWF) выявил более 132 000 веб-страниц, с подтвержденным наличием изображений и видеоматериалов, содержащих сцены сексуальных злоупотреблений в отношении детей. Каждая веб-страница могла содержать от одного до тысяч изображений этой формы злоупотреблений.

Риски, связанные с насилием в онлайновой среде, такие как распространение фотографий обнаженной натуры без согласия и кибертравля, характеризуются неравномерной гендерной динамикой, при которой девочки, как правило, в большей степени страдают от гендерно обусловленного давления в отношении сексуального поведения, испытывают более негативные последствия, сопряженные с вредом.

– Нарушения в отношении персональных данных и неправомерное их использование:

  • взлом;

  • мошенничество и кража.

  Многие люди знакомы с мошенничеством и взломом, но вторжение в частную жизнь ребенка в сети рассматривается как нарушение иного рода. Взрослые часто действуют ненадлежащим образом в отношении молодых людей, тщательно изучая содержание их мобильных телефонов и отслеживая их деятельность в сети; например, опросы детей в Бразилии показывают, что как мальчики, так и девочки из разных возрастных групп, считают, что родители более склонны контролировать использование интернета девочками. Попытки объяснить это часто указывают на то, что в некоторых случаях девочки могут быть более уязвимы из-за социальных структур, в которых они живут, в частности, с точки зрения их безопасности, в условиях, когда граница между взаимодействием в сети и в реальном мире становится все более размытой.

– Кибертравля, преследование и домогательства: враждебная и насильственная деятельность сверстников.

Чаты и сайты социальных сетей могут открыть возможность для насилия и травли, когда анонимные пользователи, в том числе молодые люди, участвуют в агрессивном или оскорбительном общении. В семи странах Европы – Бельгии, Дании, Ирландии, Италии, Португалии, Румынии и Соединенном Королевстве – Ливингстон, Маскерони, Олафссон и Хэддон[1] обнаружили, что в 2010 году в среднем 8 процентов детей стали жертвами кибертравли, а в 2014 году жертвами кибертравли стали 12 процентов детей.

Важно отметить, что дети из наиболее уязвимых групп с большей вероятностью могут стать жертвами кибертравли.

[1] Livingstone, S., Mascheroni, G., Ólafsson, K., and Haddon, L., (2014) *Children's online risks and opportunities: comparative findings from EU Kids Online and Net Children Go Mobile*. London: London School of Economics and Polilcal Science, www.eukidsonline.net and hYp://www.netchildrengomobile.eu/.

В центре внимания: усиление неравенства

В 2017 году в африканском регионе не имели доступа в сеть около 60 процентов детей, в то время как в Европе их доля составляла 4 процента. Во всех регионах мира число мужчин, пользующихся интернетом, превышает число женщин, а пользование интернетом девочками часто контролируется и ограничивается. С распространением широкополосной связи на лишенные соединений районы планеты ожидается значительное усугубление этого неравенства[15].

Дети, которые пользуются мобильными телефонами, а не компьютерами, не могут получить лучший опыт пребывания в онлайновой среде. Дети, говорящие на языках меньшинств, зачастую не могут найти нужный контент в сети, а дети из сельских районов чаще сталкиваются с кражей паролей или средств.

Исследования показывают, что многие подростки во всем мире вынуждены преодолевать существенные барьеры на пути к участию в онлайновой жизни. Для многих из них основными препятствиями остаются проблемы доступа – плохая связь, неприемлемо высокая стоимость тарифов подключения и устройств, а также отсутствие соответствующего оборудования.

С распространением доступной широкополосной связи в развивающихся странах необходимо в оперативном порядке принять меры по минимизации рисков и угроз для этих детей, а также дать им возможность воспользоваться всеми преимуществами цифрового мира.

В центре внимания: материалы, связанные с сексуальными злоупотреблениями в отношении детей (CSAM)

Масштаб проблемы

Интернет изменил масштаб и характер производства, распространения и доступности CSAM. В 2018 году технологические компании, базирующиеся в Соединенных Штатах Америки, сообщали, что во всем мире существует более 45 млн. доступных онлайновых изображений и видеоматериалов, в которых, как предполагается, дети подвергаются сексуальным злоупотреблениям. Это глобальная отрасль, и масштабы и тяжесть этого злоупотребления возрастают, несмотря на усилия по его прекращению.

Исторически сложилось так, что в реальном мире поиск CSAM для преступников был сопряжен со значительными рисками и большими затратами на доступ к материалам. Благодаря интернету преступники теперь могут относительно легко получить доступ к этим материалам и вести себя все более рискованно. Видеокамеры стали более компактными, они все больше интегрируются в каждый аспект нашей жизни, что делает процесс производства CSAM и получения контента от бесконтактных злоупотреблений легче, чем когда-либо.

Невозможно определить точный масштаб или форму этой подпольной и незаконной деятельности. Однако ясно, что количество нелегальных изображений, находящихся сейчас в обороте, может составлять миллионы. Почти все изображения с детьми были скопированы. В 2018 году IWF отследил, как часто

[15] Broadband Commission, "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online (2019)".

появлялись изображения ребенка, который был спасен в 2013 году. За три месяца аналитики IWF отследили изображения 347 раз – 25 раз в неделю.

Текущее положение дел

Каждый раз, когда изображение ребенка, подвергшегося насилию, появляется в сети или загружается преступником, этот ребенок вновь подвергается эксплуатации. Жертвы вынуждены жить с фактом продолжения существования и распространения этих изображений всю оставшуюся жизнь.

Как только обнаруживается материал, содержащий элементы сексуальных злоупотреблений в отношении детей, или веб-хостинг, на котором размещены подобные материалы, важно как можно быстрее удалить или заблокировать контент. Глобальная природа интернета усложняет эту задачу: нарушители могут производить материал в одной стране и размещать его в другой для потребителей в третьей. Практически невозможно действовать в соответствии с национальными ордерами или уведомлениями без комплексного международного сотрудничества.

Скорость инноваций в цифровом мире означает, что среда преступной деятельности постоянно меняется. Основные угрозы, которые появились в последнее время, включают:

- Повышение уровня шифрования непреднамеренно позволяет злоумышленникам действовать и обмениваться материалами по скрытым каналам, притом что обнаружение и правоохранительная деятельность усложнены.
- Форумы, посвященные грумингу детей, существуют в закрытых уголках интернета, нормализуют и поощряют такое поведение, нередко требуя загрузить новый контент для возможности присоединиться.
- Быстрое распространение интернета позволяет пользователям выходить в сеть в тех регионах, где еще только предстоит разработать/реализовать комплексную стратегию защиты или соответствующую инфраструктуру.
- Дети пользуются устройствами без присмотра во все более раннем возрасте, а сексуальное поведение в онлайновой среде нормализуется. Количество случаев злоупотребления собственноручно созданными изображениями растет с каждым годом.

В центре внимания: собственноручно созданный контент

Дети и подростки могут делать компрометирующие изображения или видеозаписи. Хотя такое поведение само по себе не обязательно является противозаконным и может иметь место в рамках нормального, здорового сексуального развития, существует риск, что любое подобное содержание может быть распространено в онлайновой среде или в реальном мире с целью причинения вреда детям или быть использовано для вымогательства. Хотя некоторые дети могут делиться своими изображениями сексуального характера в результате давления или принуждения, другие (в частности, подростки) могут с готовностью создавать сексуальный контент. Это не означает, что они соглашаются на использование и/или распространение этих изображений с целью злоупотребления или эксплуатации или несут за это ответственность.

Секстинг определяется как "самостоятельное производство изображений сексуального характера"[16], "обмен сообщениями или изображениями сексуального характера" или "создание, пересылка или рассылка непристойных изображений, изображений, содержащих обнаженную или почти обнаженную натуру, с использованием мобильного телефона и/или через интернет"[17]. Секстинг является формой самостоятельно созданного **контента** откровенного сексуального содержания[18], и эта практика "удивительно разнообразна с точки зрения контекста, значения и намерений"[19].

---

16 Karen Cooper et al., "Adolescents and Self-Taken Sexual Images: A Review of the Literature", *Computers in Human Behaviour* 55 (February 2016): 706–16, https://doi.org/10.1016/j.chb.2015.10.003.

17 Jessica Ringrose et al., "A Qualitative Study of Children, Young People and "Sexting": A Report Prepared for the NSPCC" (London, UK: National Society for the Prevention of Cruelty to Children, 2012), http://doi.wiley.com/10.1046/j.1365-2206.1997.00037.x.

18 UNODC, "Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children" (Vienna: UN, 2015), https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf.[3] UNODC, Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children, p. 22.

19 Cooper et al., "Adolescents and Self-Taken Sexual Images".

Хотя секстинг, возможно, является наиболее распространенной формой откровенного сексуального контента, создаваемого самими детьми, и часто происходит по обоюдному согласию подростков, которые получают удовольствие от опыта, существует также много форм непрошенного секстинга. Речь идет об аспектах этой деятельности, в которых отсутствует элемент согласия, таких как обмен или получение нежелательных откровенных фотографий, видеозаписей или сообщений, например, от известных или неизвестных лиц, пытающихся вступить в контакт с ребенком, оказать на него давление или обхаживать его. Секстинг также может быть формой травли сексуального характера, когда на ребенка оказывают давление, чтобы он отправил фотографию парню/подруге/сверстнику, которые затем распространяют ее среди сверстников без получения согласия.

В центре внимания: кибертравля

В то время как травля как явление появилась задолго до интернета, выросшие масштабы, сфера охвата и непрерывность травли, совершаемой в онлайновой среде, могут еще больше усугубить и так неприятный и зачастую вредный опыт для жертв. Кибертравля определяется как умышленное и неоднократное нанесение вреда посредством использования компьютеров, мобильных телефонов и других электронных устройств. Она часто имеет место параллельно с травлей в реальном мире, происходящей в школе или где-либо еще, может иметь дополнительные расистские, религиозные или сексистские аспекты, и представлять собой продолжение вреда, причиняемого в онлайновой среде например, посредством взлома учетной записи, распространения фотографий и видео в сети, а также непрерывного характера оскорбительных сообщений и доступности контента. Как правило, это проблема социального характера, не имеющая элементов уголовно наказуемого деяния, и стратегия борьбы с явлением кибертравли требует целостного подхода, охватывающего школы, семьи и, в первую очередь, самих детей.

В центре внимания: груминг и секс-вымогательство в онлайновой среде

С быстрым развитием технологий и расширением доступа к интернету и цифровым средствам связи, наблюдаемым в последние годы, неизбежно растет риск совершения в интернете преступных деяний, направленных против детей. Среди этих новых форм сексуальной эксплуатации детей в сети можно назвать груминг и секс-вымогательство в отношении детей в онлайновой среде. Груминг в онлайновой среде в широком смысле означает процесс установления дружеских отношений взрослого с ребенком (в возрасте до 18 лет) и оказания влияния на ребенка посредством использования интернета или других цифровых технологий для облегчения контактного или бесконтактного сексуального взаимодействия с этим ребенком. В процессе груминга нарушитель пытается добиться выполнения ребенком инструкций, чтобы сохранить тайну и избежать обнаружения и наказания[20]. Важно признать, что существуют также случаи злоупотреблений между сверстниками.

По данным Интерпола, интернет облегчает груминг благодаря наличию большого числа легкодоступных потенциальных целей и возможности для грумеров представляться привлекательным для ребенка образом. Нарушители, занимающиеся сексуальной эксплуатацией детей в онлайновой среде, используют манипуляцию, принуждение и соблазн, чтобы преодолеть сдерживающие факторы и соблазнить детей к участию в действиях сексуального характера. Грумер преднамеренно выявляет уязвимую потенциальную жертву, собирает информацию о ситуации в семье ребенка и использует давление или чувство стыда/страха для сексуальной эксплуатации ребенка. Грумеры могут использовать порнографические материалы для взрослых, а также контент, содержащий элементы насилия над детьми или их эксплуатации, чтобы преодолеть сдерживающие факторы поведения потенциальных жертв, представляя участие ребенка в действиях сексуального характера как естественное и нормальное. Интернет изменил способ взаимодействия людей друг с другом, и дал новое определение понятию "друг". Грумер может очень легко и быстро установить дружбу с ребенком в онлайновой среде, что заставляет пересмотреть традиционные образовательные сообщения об опасностях, исходящих от незнакомцев.

Груминг в онлайновой среде был впервые официально признан в **Конвенцией Совета Европы о защите детей от сексуальной эксплуатации и сексуальных злоупотреблений** (Лансаротская конвенция) – международном правовом документе 2007 года. Статья 23 устанавливает уголовную ответственность за "домогательство в отношении детей с сексуальными целями", которая предполагает наличие умышленного предложения встретиться с ребенком с целью совершения преступления сексуального характера, за которым следуют "практические действия, направленные на проведение такой встречи". Во

[20] International Centre for Missing & Exploited Children, "Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review", 1st Edition (International Centre for Missing & Exploited Children, 2017), https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf.

многих случаях груминга дети подвергаются сексуальным злоупотреблениям и сексуальной эксплуатации в онлайновой среде – "встреча", предусмотренная Лансаротской конвенцией и многими существующими национальными законами, является полностью виртуальной, но, тем не менее, наносит такой же вред ребенку, как и встреча в реальном мире. Крайне важно, чтобы уголовная ответственность за груминг распространялась "на случаи, когда сексуальные злоупотребления не являются результатом личной встречи, а совершается в онлайновой среде"[21].

Секс-вымогательство может иметь место как часть груминга в онлайновой среде или как самостоятельное преступление[22]. Хотя секс-вымогательство может происходить отдельно от груминга в онлайновой среде, в некоторых случаях груминг в онлайновой среде может привести к секс-вымогательству[23]. Секс-вымогательство может происходить в контексте груминга в онлайновой среде, так как грумер манипулирует ребенком и оказывает на него влияние в процессе груминга, угрожая, запугивая и принуждая его пересылать свои изображения сексуального характера (собственноручно созданный контент)[24]. Если жертва не предоставляет запрошенные сексуальные услуги, дополнительные интимные изображения, деньги или другие услуги, ее изображения могут быть размещены в интернете с целью унизить, вызвать тревогу или принудить ребенка к созданию дополнительного контента откровенно сексуального характера[25].

Секс-вымогательство классифицируется как "виртуальное насильственное действие сексуального характера" из-за схожих эмоциональных и психологических последствий для жертв[26]. В некоторых случаях действие настолько травмирует, что жертвы пытались причинить себе вред или совершить самоубийство, чтобы избежать злоупотреблений.

Европол отмечает, что сбор информации для оценки масштаба секс-вымогательства, затрагивающего детей, является сложной задачей и этот масштаб может быть сильно занижен[27]. Кроме того, отсутствие общей терминологии и определений для груминга и секс-вымогательства в онлайновой среде является препятствием для сбора точных данных и понимания истинного масштаба проблем во всем мире.

2.6 Дети, находящиеся в уязвимом положении

Дети и молодые люди могут находиться в уязвимом положении по целому ряду причин. Исследование, проведенное в 2019 году, показало, что "жизнь в цифровой среде детей и молодых людей, находящихся в уязвимом положении, не сопровождается тем особым и внимательным отношением, которое в реальной жизни обусловливается их неблагоприятной ситуацией. Более того, в отчете далее говорится, что "в лучшем случае они [дети и молодые люди] получают те же общие советы по безопасности в онлайновой среде, что и все остальные дети и молодые люди, в то время как им требуется специализированная помощь".

Здесь рассматриваются три конкретные категории детей в уязвимом положении (дети мигранты, дети с расстройствами аутистического спектра и дети-инвалиды), однако их существует значительно больше.

Дети-мигранты

Дети и молодые люди из среды мигрантов часто приезжают в страну (или уже живут там) с определенным социокультурным опытом и ожиданиями. Несмотря на то что технологии обычно рассматриваются как

---

21 Lanzarote Committee, Committee of the Parties to the Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse, *Solicitation of children for sexual purposes through information and communication technologies (grooming), Opinion on Article 23 of the Lanzarote Convention and its explanatory note*, Jun. 17, 2015, *at* ***https://edoc.coe.int/en/children-s-rights/7064-lanzarote-committee-opinion-on-article-23-of-the-lanzarote-convention-and-its-explanatory-note.html*** (last visited Nov. 6, 2019).

22 National Center for Missing and Exploited Children (NCMEC), *Sextortion*, *at* http://www.missingkids.com/theissues/onlineexploitation/sextortion (last visited Nov. 6, 2019).

23 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, Interagency Working Group in Sexual Exploitation of Children, Luxembourg, Jan. 28, 2016, D.4iii, 27–28, *at* http://luxembourgguidelines.org/english-version.

24 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, Interagency Working Group in Sexual Exploitation of Children, Luxembourg, Jan. 28, 2016, D.4iii, 27–28, *at* http://luxembourgguidelines.org/english-version.

25 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, Interagency Working Group in Sexual Exploitation of Children, Luxembourg, Jan. 28, 2016, D.4iii, 27–28, *at* http://luxembourgguidelines.org/english-version.

26 Benjamin Wittes et al., "Sextortion: Cybersecurity, Teenagers, and Remote Sexual Assault" (Brookings Institution, May 11, 2016), https://www.brookings.edu/wp-content/uploads/2016/05/sextortion1-1.pdf.

27 Europol, "Online Sexual Coercion and Extortion as a Form of Crime Affecting Children: Law Enforcement Perspective" (European Cybercrime Centre, May 2017), https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf.

фактор, способствующий налаживанию связей и общественному участию, уровень онлайновых рисков и возможностей может значительно варьироваться в зависимости от условий. Кроме того, полученные эмпирическим путем данные и практические исследования свидетельствуют о важнейшей роли цифровых средств в целом:

- Они важны для целей ориентирования (при переезде в новую страну).
- Это важнейшее средство освоения и ознакомления с обществом/культурой принимающей страны.
- Социальные сети могут играть ключевую роль в поддержании связи с семьей и сверстниками, а также в получении доступа к информации общего характера.

Наряду со многими положительными аспектами цифровые средства могут также создавать для мигрантов трудности:

- Инфраструктура: важно задумываться о создании безопасного онлайнового пространства, для того чтобы дети и молодые люди – мигранты могли пользоваться интернетом безопасно и конфиденциально.
- Ресурсы: мигранты тратят большую часть денег на телефонные карты с предварительной оплатой.
- Интеграция: наряду с доступом к технологиям детям и молодым людям – мигрантам также необходимо хорошее цифровое образование.

Дети с расстройствами аутистического спектра (ASD)

Аутистический спектр охватывает две из основных областей поведенческой диагностической классификации DSM-5:

- ограниченное и повторяющееся поведение ("потребность в однообразии");
- трудности общения и коммуникации;
- частая встречаемость в сочетании с умственной отсталостью, языковыми и аналогичными проблемами

Технологии и интернет открывают детям и молодым людям безграничное число возможностей для обучения, общения и игр. Однако наряду с преимуществами имеется значительное количество рисков, которым могут быть в большей степени подвержены дети и молодые люди с ASD:

- Интернет может дать детям и молодым людям с аутизмом возможности в сфере социализации и реализации особых интересов, которых у них может не быть в реальной жизни.
- Проблемы социального характера, такие как трудности в понимании намерений других людей, могут привести к тому, что представители этой группы окажутся уязвимы перед "друзьями" с недобрыми намерениями.
- Проблемы, возникающие в онлайновой среде, нередко обусловлены основными характерными особенностями аутизма: конкретные и точные руководящие указания могут способствовать адаптации этих лиц к онлайновой среде, однако их базовые проблемы сохранятся.

Дети-инвалиды

Дети-инвалиды сталкиваются с рисками в онлайновой среде во многом так же, как и дети без инвалидности, но помимо этого они могут сталкиваться со специфическими рисками, связанными с их инвалидностью. Дети-инвалиды нередко сталкиваются с маргинализацией, стигматизацией и барьерами (физическими, экономическими, социальными, а также касающимися отношения со стороны других) для участия в жизни своих сообществ. Подобный опыт может способствовать тому, что ребенок-инвалид будет стремиться к социальному взаимодействию и поиску друзей в онлайновой среде, что может иметь положительный результат, повысить самооценку и привести к созданию сетей поддержки. Вместе с тем это может привести к повышенному риску таких действий в отношении этих детей и молодых людей как груминг, склонение в онлайновой среде к действиям сексуального характера и/или сексуальные домогательства. Согласно исследованиям, дети и молодые люди, имеющие сложности в реальном мире, а также испытывающие проблемы психологического характера, подвергаются повышенному риску подобных инцидентов[28].

[28] Andrew Schrock et al., "Solicitation, Harassment, and Problematic Content", *Berkman Center for Internet & Society, Harvard University*, December 2008, 87, https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF-LitReviewDraft_0.pdf.'

В целом, дети, которые становятся жертвами в реальном мире, скорее всего, будут жертвами в онлайновой среде. Это означает, что дети-инвалиды подвержены более высокому риску в онлайновой среде, притом что они испытывают в ней бóльшую потребность. Исследования показывают, что дети-инвалиды чаще становятся жертвами злоупотреблений любого рода[29] и, в частности, сексуальной виктимизации[30]. Виктимизация может включать в себя травлю, домогательства, исключение и дискриминацию, основанную на фактической или предполагаемой инвалидности ребенка, или на аспектах, связанных с инвалидностью, например, особенностями его поведения или речи, используемыми им оборудованием или услугами.

Среди лиц, совершающих такие правонарушения как груминг, склонение в онлайновой среде к действиям сексуального характера и/или сексуальные домогательства в отношении детей и молодых людей – инвалидов, могут быть не только нарушители, выбирающие своими жертвами именно детей и молодых людей, но также и те, которые выбирают именно детей и молодых людей – инвалидов. К таким нарушителям относятся так называемые "девоти" – люди без инвалидности, испытывающие сексуальное влечение к людям-инвалидам (как правило, к лицам с ампутированными конечностями или лицам, передвигающимся при помощи средств, облегчающих мобильность), причем некоторые из них сами притворяются инвалидами[31]. Подобные люди могут совершать такие действия, как загрузка фото и видео детей и молодых людей с инвалидностью (которые сами по себе безвредны) и/или их распространение через специально создаваемые форумы и учетные записи в социальных сетях. Механизмы информирования в рамках форумов и социальных сетей часто не предусматривают возможностей пресечения подобных действий.

Возникают опасения, что "шарентинг" (англ. "sharenting" – размещение родителями данных и фотографий своих детей в интернете) может нарушить право ребенка на неприкосновенность частной жизни, привести к травле, возникновению неловких ситуаций или негативно отразиться на дальнейшей жизни[32]. Родители детей-инвалидов иногда делятся такой информацией в поисках содействия или совета, тем самым подвергая детей-инвалидов более высокому риску негативных последствий.

Некоторые дети-инвалиды могут сталкиваться с трудностями при использовании онлайновых площадок или даже с исключением из сетевой среды из-за недоступного дизайна (например, приложения, которые не позволяют увеличить размер текста), отсутствия специальных возможностей (например, программного обеспечение для чтения с экрана или адаптивного компьютерного управления) или необходимости в соответствующей поддержке (например, обучения использованию оборудования, помощи с ориентированием в социальных взаимодействиях[33]).

В отношении риска, связанного с заключением договора или подписанием условий, дети-инвалиды в большей степени рискуют принять юридические условия, которые иногда не могут понять даже взрослые.

2.7 Восприятие детьми рисков в онлайновой среде

Дети обращают внимание на такие риски, как подверженность насилию во всем мире, доступ к неприемлемому контенту, товарам и услугам; обеспокоенность по поводу чрезмерно активного пользования продуктами; вопросы защиты данных и неприкосновенности частной жизни[34].

Подростки сообщают о целом ряде проблем, связанных с их взаимодействием с цифровыми технологиями. К ним относятся широко обсуждаемые проблемы безопасности в онлайновой среде, такие как опасения взаимодействия с незнакомыми людьми в сети, доступ к неподходящему контенту или воздействие

---

29 UNICEF, "State of the World's Children Report: Children with Disabilities", 2013, https://www.unicef.org/publications/files/SOWC2013_Exec_Summary_ENG_Lo_Res_24_Apr_2013.pdf.

30 Katrin Mueller-Johnson, Manuel P. Eisner, and Ingrid Obsuth, "Sexual Victimization of Youth with a Physical Disability: An Examination of Prevalence Rates, and Risk and Protective Factors", *Journal of Interpersonal Violence* 29, № 17 (November 2014): 3180–3206, https://doi.org/10.1177/0886260514534529.

31 Richard L Bruno, "Devotees, Pretenders and Wannabes: Two Cases of Factitious Disability Disorder", *Sexual and Disability* 15, № 4 (1997): 18, https://link.springer.com/content/pdf/10.1023/A:1024769330761.pdf.

32 UNICEF, "Child Privacy in the Age of Web 2.0 and 3.0: Challenges and Opportunities for Policy", Innocenti Discussion Paper 2017-03 (UNICEF, Office of Research-Innocenti), дата обращения: 16 января 2020 года, https://www.unicef-irc.org/publications/pdf/Child_privacy_challenges_opportunities.pdf.

33 Руководящие указания по этим правам изложены в Статье 9 о доступности и Статье 21 о свободе выражения мнений и доступе к информации Конвенции о правах инвалидов.

34 Amanda Third et al., "Children's Rights in the Digital Age" (Melbourne: oung and Well Cooperative Research Centre, September 2014), http://www.uws.edu.au/__data/assets/pdf_file/0003/753447/Childrens-rights-in-the-digital-age.pdf.

вредоносных программ или вирусов, в то время как другие проблемы связаны с надежностью их доступа к технологиям: вторжение родителей в их "частную" жизнь в сети, их навыки цифровой грамотности[35].

Исследование EU Kids Online показывает, что порнография и содержание, содержащее насилие, являются главными проблемами детей в онлайновой среде в Европе. В целом, мальчиков больше беспокоит насилие, в то время как девочек больше беспокоят риски, связанные с контактами[36]. Опасения по поводу рисков выше среди детей из стран с "активным пользованием, высоким уровнем риска".

В Латинской Америке консультации с детьми показали, что основными проблемами, вызывающими обеспокоенность, являются утрата неприкосновенности частной жизни, насилие и домогательства[37]. Дети сообщают о том, что с ними связывались незнакомые им люди – это особенно актуально в онлайновых играх. В таких ситуациях основная стратегия, по всей видимости, не реагировать на незнакомца и/или блокировать контакт. Девочки сталкиваются с домогательствами в социальных сетях с раннего возраста. Им удается самостоятельно ориентироваться в этих формах насилия, блокируя пользователей и изменяя настройки конфиденциальности. Домогательства исходят от пользователей, которые иногда не говорят по-испански, но успевают отправить им изображения, попросить добавить в друзья и прокомментировать их сообщения. Некоторые мальчики также сообщают о получении таких запросов.

Во многих частях мира дети хорошо понимают некоторые риски, с которыми они сталкиваются в сети[38]. Исследования показали, что большинство детей способны отличить кибертравлю от шуток и поддразнивания в онлайновой среде, понимая, что кибертравля имеет общественное измерение и направлена на нанесение вреда[39].

3 Подготовка национальной стратегии защиты ребенка в онлайновой среде

При разработке национальной стратегии защиты ребенка в онлайновой среде для содействия безопасности детей и молодых людей в онлайновой среде, национальные правительства и директивные органы должны выявлять передовой опыт и взаимодействовать с основными заинтересованными сторонами.

В нижеследующих разделах представлены типичные участники и заинтересованные стороны, а также описание их потенциальной роли и возможных обязанностей в отношении защиты детей в онлайновой среде.

3.1 Участники и заинтересованные стороны

Директивные органы могут определять подходящих лиц, группы и организации, представляющие каждую из этих структур и заинтересованных сторон в пределах своей компетенции. Для координации и организации деятельности на национальном уровне в рамках стратегий защиты ребенка в онлайновой среде важно осуществить оценку текущих, планируемых и потенциальных мероприятий.

Дети и молодые люди

Во всем мире дети и молодые люди продемонстрировали, что они очень легко могут адаптироваться к новым технологиям и использовать их. Важность интернета для школ растет, и он становится площадкой, где дети могут играть, работать и общаться.

---

35 Amanda Third et al., "Young and Online: Children's Perspectives on Life in the Digital Age", The State of the World's Children 2017 Companion Report (Sydney: Western Sydney University, 2017). The report summarized the views of 490 children aged 10–18, from 26 different countries speaking 24 official languages.

36 Livingstone, S. (2014) *EU Kids Online: Findings, methods, recommendations*. LSE, London: EU Kids Online, https://lsedesignunit.com/EUKidsOnline/.

37 Conectados al Sur network, "Hablatam".

38 С 2016 года МСЭ проводит консультации по тематике СОР с участием детей и представляющих заинтересованные стороны взрослых, затрагивая такие вопросы, как кибертравля, цифровая грамотность и деятельность детей в сети.

39 UNICEF, "Global Kids Online Comparative Report (2019)".

Согласно последнему отчету Альянса "ChildFund", только 18,1 процента опрошенных детей считают, что директивные органы действуют в целях их защиты. Важно, чтобы директивные органы взаимодействовали с детьми в этом отношении, признавая их право быть выслушанными (Статья 12 КПР).

Для того чтобы иметь возможность защитить детей, директивные органы должны стандартизировать определение понятия "ребенок" во всех правовых документах. Под ребенком должно пониматься любое лицо в возрасте до 18 лет. Это соответствует Статье 1 Конвенции ООН о правах ребенка (КПР ООН), которая гласит, что "ребенок означает любое человеческое существо, не достигшее 18 лет". Не следует позволять компаниям считать взрослым любого человека, не достигшего 18 лет, но юридически достаточно взрослого для того, чтобы дать согласие на обработку данных. Такое узкое определение не подтверждено никакими доказательствами в отношении этапов развития ребенка. Оно подрывает права детей и угрожает их безопасности.

В то время как может казаться, что многие дети уверенно используют технологии, многие не чувствуют себя в сети в безопасности[40] и имеют некоторые опасения[41] относительно интернета.

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 сети, и то, что там происходит на самом деле, может совершенно не совпадать. Половина всех опрошенных детей сказали, что в их стране взрослые не прислушиваются к их мнению по вопросам, которые их волнуют[42]. По этой причине важно, чтобы независимо от того, какие меры принимаются на национальном уровне для разработки политики в этой области, были найдены соответствующие механизмы, позволяющие всем детям и молодым людям быть услышанными, и чтобы был учтен их конкретный опыт использования технологий.

Родители, опекуны и педагоги

Родители, опекуны и педагоги проводят больше всего времени с детьми. Они должны быть обучены цифровой грамотности, чтобы понимать онлайновую среду и уметь защищать детей и научить их, как защитить себя.

Образовательные учреждения несут особую ответственность за обучение детей тому, как быть в большей безопасности в сети, независимо от того, используют ли они интернет в школе, дома или где-либо еще, а директивные органы должны включать в национальные учебные программы вопросы цифровой грамотности с самого раннего возраста (от 3 до 18 лет). Это позволило бы детям иметь возможность защищать себя, знать свои права и, следовательно, использовать интернет как средство, способствующее получению знаний[43].

Директивные органы должны иметь в виду, что родители и опекуны почти всегда будут первой, последней и лучшей линией обороны и поддержки для собственных детей. Однако, когда речь заходит об интернете, они могут почувствовать себя несколько неуверенно. Опять же, школа может стать важным каналом связи с родителями и опекунами, чтобы они знали как о рисках, так и о многих возможностях, которые предоставляют новые технологии. Однако школы не должны стать единственным каналом информирования родителей и опекунов. Важно использовать множество различных путей, чтобы максимизировать возможность обращения к максимально возможному числу родителей и опекунов. Компании отрасли играют здесь важную роль, осуществляя поддержку своих пользователей или клиентов. Родители и опекуны могут выбрать управление деятельностью своего ребенка в сети и доступ к ней, поговорить с ребенком о правильном поведении и использовании технологий, понять, что ребенок делает в сети, чтобы семейный разговор объединил в себе опыт онлайновой среды и реального мира.

---

40 ChildFund Alliance, "VIOLENCE AGAINST CHILDREN AS EXPLAINED BY CHILDREN", Save Voices Big Dreams, 2019, https://childfundalliance.org/zdocs/a9357061-749f-4ebf-a1e9-b1aee81cb216/SVBD-THE_REPORT-digital.pdf.

41 Council of Europe, "It's Our World: Children's Views on How to Protect Their Rights in the Digital World", Report on child consultations (Council of Europe, Children's Right Division, October 2017), https://rm.coe.int/it-s-our-world-children-s-views-on-how-to-protect-their-rights-in-the-/1680765dff.

42 ChildFund Alliance, "Violence against children as explained by children".

43 UNICEF, "Policy Guide on Children and Digital Connectivity" (Policy Lab, Data, Research and Policy, United Nations Children's Fund, June 2018), https://www.unicef.org/esa/media/3141/file/PolicyLab-Guide-DigitalConnectivity-Nov.6.18-lowres.pdf.

Родители и опекуны также должны подавать хороший пример своим детям в том, как пользоваться своими устройствами и правильно вести себя в интернете.

Директивные органы должны помнить, что с родителями и опекунами следует консультироваться для выяснения их мнений, опыта и формирования у них понимания необходимости защиты их детей в онлайновой среде.

Наконец, директивные органы совместно с другими государственными учреждениями могут разрабатывать кампании по информированию общественности, в том числе для родителей, опекунов и педагогов. Публичные библиотеки, медицинские центры, даже торговые центры и другие крупные центры розничной торговли могут предоставить доступные помещения для презентации информации об электронной безопасности и цифровых навыках. Выполняя эту задачу, правительства должны обеспечить нейтральность даваемых рекомендаций, свободу от любых частных интересов, а также они должны охватывать широкий спектр вопросов в рамках цифрового пространства.

Компании отрасли

Компании отрасли являются одной из ключевых заинтересованных сторон в экосистеме, поскольку они обладают технологическими знаниями, которые директивные органы должны учитывать и понимать для развития правовой базы. Таким образом, по сути дела, директивные органы вовлекают **компании отрасли** в процесс разработки законов о защите ребенка в онлайновой среде.

Кроме того, при разработке новых технологий важно поощрять **компании отрасли** внедрять подходы, основанные на учете задачи обеспечения безопасности на этапе проектирования. Очевидно, что компании, разрабатывающие или предоставляющие новые технологические продукты и услуги, должны помогать своим пользователям понять, как они работают, и как безопасно и правильно их использовать.

Компании отрасли также несут основную ответственность за содействие повышению осведомленности о программе действий по безопасности и онлайновой среде, в частности, для детей и их родителей или опекунов, а также для сообщества в целом. Участвуя в этой работе, заинтересованные стороны отрасли узнают больше о проблемах, вызывающих обеспокоенность других заинтересованных сторон, а также о рисках и вреде, которым подвергаются конечные пользователи. Обладая такими знаниями, **компании отрасли** могут корректировать существующие продукты и услуги и выявлять опасности на этапе разработки.

Последние достижения в области искусственного интеллекта формируют возможность для компаний отрасли создать более надежную систему сдержек и противовесов для идентификации пользователя и обеспечения детей благоприятной средой для конструктивного поведения в онлайновой среде. Эти достижения также могут представлять для детей новые риски.

В ряде странах интернет управляется в рамках парадигмы саморегулирования или совместного регулирования. Тем не менее, некоторые страны рассматривают или уже внедрили нормативно-правовую базу, включая обязательства компаний по выявлению, блокированию и/или удалению источников вреда в отношении детей с платформ или услуг, а также по предоставлению четких механизмов подачи жалоб и доступа к поддержке.

Академическое сообщество и неправительственные организации

В университетах и академическом сообществе, скорее всего, имеется целый ряд ученых и исследователей, которые профессионально интересуются социальным и техническим воздействием интернета и обладают весьма обширными знаниями в этой области. Они являются очень ценным ресурсом с точки зрения оказания помощи национальным правительствам и директивным органам в формулировании стратегий, основанных на неопровержимых фактах и убедительных доказательствах. Они также могут выступать в качестве интеллектуального противовеса бизнес-интересам, которые иногда могут быть слишком краткосрочными и ориентированными на прибыль.

Аналогичным образом, в сообществе неправительственных организаций (НПО) есть целый ряд носителей экспертных знаний и информации, которые могут быть неоценимым ресурсом предоставлении услуг детям, родителям, опекунам и педагогам для содействия продвижению повестки дня в области защиты в онлайновой среде и, в более общем плане, защиты общественных интересов.

Органы охраны правопорядка

Очень печально, что такая замечательная технология привлекает также внимание криминальных и антисоциальных элементов. Интернет значительно увеличил объемы оборота CSAM и других источников вреда в сети. Сексуальные хищники используют интернет для первого контакта с детьми, заманивая их в очень вредные формы контакта, как в онлайновой среде, так и в реальном мире. Травля и другие формы преследования могут нанести большой вред жизни детей, и интернет открыл для этого новый путь.

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 правоохранительных органов должны пройти надлежащую подготовку для проведения расследований связанных с интернетом преступлений против детей и молодых людей. Им необходим надлежащий уровень технических знаний и доступ к инструментам криминалистики, чтобы они могли извлекать и интерпретировать данные, полученные с компьютеров или из сети, за минимальное время.

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 CSAM, и существуют аналогичные специальные механизмы для упрощения передачи сообщений о других видах проблем, например, о травле. Директивным органам следует сотрудничать с Международной ассоциацией горячих линий интернета (INHOPE), оказывая им поддержку в оценке и обработке отчетов о CSAM, и извлекать пользу из оказания поддержки INHOPE организациям по всему миру в создании "горячей линии" там, где ее нет. Директивные органы должны обеспечить наличие открытых каналов связи между правоохранительными органами и другими заинтересованными сторонами. Правоохранительные органы являются основным источником CSAM, изымаемого в пределах национальных границ. Необходимо организовать процесс изучения этих материалов, чтобы установить, можно ли идентифицировать местных жертв. Там, где это невозможно, материалы следует передать в Интерпол для включения в базу данных ICSE. Поскольку это угроза глобального масштаба, директивные органы должны обеспечить международное сотрудничество между правоохранительными органами во всем мире. Это сократит время формальных процессов и позволит агентам быстрее реагировать.

Социальные службы

Там, где дети или молодые люди испытывали вредные воздействия или подверглись злоупотреблениям 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. Может также возникнуть необходимость в комплексной психологической помощи и методах восстановления для правонарушителей, особенно для несовершеннолетних правонарушителей, которые, возможно, также стали жертвами злоупотреблений в сети или в реальном мире. Профессионалы, работающие в социальных службах, должны быть соответствующим образом обучены, для того чтобы иметь возможность предоставить поддержку такого вида. Поддержку следует оказывать в онлайновом режиме и обычными способами.

Службы здравоохранения

Медицинская помощь, необходимая после любого случая насилия в отношении ребенка, должна быть включена в базовый план медицинского обслуживания на национальном уровне. Медицинские учреждения должны в обязательном порядке сообщать о случаях жестокого обращения. Медицинские работники должны быть надлежащим образом оснащены и осведомлены, чтобы иметь возможность оказывать поддержку детям в этом отношении. Медицинские услуги должны распространяться на поддержку психического здоровья и благополучия детей.

Правительственные учреждения

Политика защиты ребенка в онлайновой среде будет находиться в ведении ряда правительственных учреждений, и важно задействовать их все для успешной реализации любой национальной стратегии и плана действий. Они могут включать:

- министерство внутренних дел;

- министерство здравоохранения;
- министерство образования;
- министерство юстиции;
- министерство цифрового развития/информации;
- регуляторные органы.

Регуляторные органы имеют наилучшие возможности для того, чтобы выполнять задачи контроля и учета в сотрудничестве с правительственными учреждениями. Сюда могут входить органы, регулирующие средства массовой информации и защиту данных.

Операторы широкополосных, мобильных и Wi-Fi сетей

Операторы могут обнаруживать, блокировать незаконный контент в своей сети и сообщать о нем, а также предоставлять инструменты, услуги и конфигурации для использования семьями и родителями при выборе способа управления доступом своих детей. Важно, чтобы поставщики услуг в равной степени обеспечивали соблюдение гражданских свобод и неприкосновенность частной жизни.

Права ребенка

Независимые организации, занимающиеся защитой прав ребенка, могут играть решающую роль в обеспечении защиты детей в интернете. Хотя их полномочия варьируются, такие учреждения решают, как правило, следующие задачи:

- следить за воздействием законодательства, политики и правоприменения на защиту прав ребенка;
- содействовать реализации международных стандартов в области прав человека на национальном уровне;
- расследовать нарушения прав ребенка;
- представлять экспертное знание в области прав ребенка в судах;
- обеспечить заслушивание мнений детей по вопросам, касающимся их прав человека, включая разработку соответствующих законов и политики;
- содействовать пониманию и осознанию общественностью прав ребенка; и
- предпринимать инициативы по обучению и подготовке специалистов в области прав человека.

Важно включить прямые консультации с детьми, поскольку это их право в соответствии со Статьей 12 КПР ООН. Консультативные, следственные, информационные и образовательные функции независимых правозащитных учреждений для детей имеют важное значение для предотвращения вреда в онлайновой среде и реагирования на него. По этой причине такие учреждения должны активно участвовать в разработке всеобъемлющего, основанного на правах подхода к укреплению правовых, нормативных и политических рамок, регулирующих защиту ребенка в онлайновой среде, включая прямые консультации с детьми, поскольку это их право в соответствии со Статьей 12 КПР ООН.

В последнее время также были примеры, когда в государствах создавались государственные учреждения, наделенные конкретными полномочиями по поддержке прав ребенка в сети, включая их защиту от насилия или источников вреда, или рассматривались возможности их создания. Там, где существуют такие учреждения, они также должны быть тесно связаны с мерами по усилению реагирования в целях защиты ребенка в онлайновой среде на национальном уровне.

3.2 Существующие ответные меры по защите ребенка в онлайновой среде

Был разработан ряд инициатив, направленных на то, чтобы действовать на национальном и международном уровнях с учетом возрастающего значения ИКТ в жизни детей во всем мире и присущих им рисков для самых младших членов наших обществ.

Национальные модели

На национальном уровне следует выделить несколько законодательных инициатив, охватывающих важные аспекты всеобъемлющей рамочной основы защиты ребенка в онлайновой среде. Они включают, среди прочих, следующие:

- Директива об аудиовизуальных медиа-услугах (AVMSD) (пересм. 2018 г., ЕС);
- Общий регламент о защите данных (GDPR) (2018 г., ЕС).

В нормативно-правовом и институциональном реагировании государств-членов на угрозы безопасности и благополучию детей в сети есть инновационные решения. Единого способа реагирования на CSAM, кибертравлю и другие источники вреда, с которыми дети сталкиваются в онлайновой среде, не существует, однако следует отметить, что за последние несколько лет были опробованы новые подходы:

Кодекс проектирования с учетом возраста (2019 г., Соединенное Королевство)

В начале 2019 года Управление Комиссара по информации опубликовало в интернете предложения по своему "кодексу проектирования с учетом возраста" для укрепления защиты детей. В предлагаемом кодексе основное внимание уделяется наилучшему обеспечению интересов ребенка, как это предусмотрено в КПР ООН, и излагается ряд ожиданий, возлагаемых на компании отрасли. К ним относятся надежные меры по проверке возраста, отключение по умолчанию услуги по определению местонахождения для детей, сбор и хранение компаниями только минимального объема персональных данных детей, продуманная безопасность продуктов, доступность и соответствие возрасту объяснений.

Закон о вредоносной цифровой коммуникации (пересм. 2017 г., Новая Зеландия)

В законе 2015 года вводится уголовная ответственность за злоупотребление ИКТ; основное внимание уделено широкому диапазоне видов ущерба, от кибертравли до распространения материалов порнографического содержания из соображений мести. Закон направлен на сдерживание, предотвращение и уменьшение вредоносного цифрового общения, запрещая размещение цифрового сообщения с намерением причинить значительные эмоциональные страдания кому-либо другому, и устанавливает 10 принципов общения. Он уполномочивает пользователей подавать жалобы в независимую организацию, если эти принципы нарушаются, или ходатайствовать о судебном постановлении в отношении автора или разместившей сообщение структуры, если вопрос не решен.

Комиссариат по электронной безопасности (2015 г., Австралия)

Комиссариат по вопросам электронной безопасности (eSafety) – это первое в мире правительственное учреждение, специализирующееся на безопасности в онлайновой среде. Учрежденная в 2015 году структура имеет законодательно закрепленные функции по руководству, координации, обучению и консультированию по вопросам безопасности в онлайновой среде, чтобы обеспечить всем гражданам Австралии безопасный, позитивный и расширяющий их возможности опыт работы в сети. eSafety проводит расследования, касающиеся значительных источников вреда, включая серьезную кибертравлю детей, жестокое обращение с использованием изображений и запрещенный контент. Структура уполномочена проводить расследования и принимать меры для рассмотрения жалоб или сообщений, касающихся такого вреда, включая, в некоторых случаях, полномочия по направлению уведомлений отдельным лицам и онлайновым службам для удаления материалов. Наряду с полномочиями по проведение расследований, eSafety применяет комплексный подход, основанный на социальных, культурных и технологических инициативах и действиях. Ее усилия по профилактике и защите и активный подход обеспечивают комплексное решение вопроса безопасности в онлайновой среде.

Международные модели

На международном и транснациональном уровнях различными заинтересованными сторонами были разработаны рекомендации и стандарты. Настоящие руководящие указания основаны на результатах работы, проделанной в рамках следующих усилий:

Руководящие указания, касающиеся осуществления Факультативного протокола к Конвенции о правах ребенка, касающегося торговли детьми, детской проституции и детской порнографии.

Руководящие указания Совета Европы по уважению, защите и реализации прав ребенка в цифровой среде[44].

Руководящие указания адресованы всем государствам – членам Совета Европы с целью оказания помощи Государствам-Членам и другим соответствующим заинтересованным сторонам в их усилиях по принятию комплексного стратегического подхода к максимальному соблюдению всего спектра прав детей в цифровой среде. Среди многих рассматриваемых тем – защита персональных данных, предоставление адаптированного к потребностям и развивающимся способностям детей контента, телефоны доверия и "горячие линии", уязвимость и адаптация, а также роль и ответственность компаний. Кроме того, в руководящих указаниях содержится призыв в адрес государств взаимодействовать с детьми, в том числе в процессе принятия решений, для должного отражения изменений в цифровой среде в национальной политике. В настоящее время руководящие принципы доступны на 19 языках. Они будут сопровождаться адаптированной для детей версией документа, а также Руководством для директивных органов, в котором будут изложены конкретные меры по реализации этих руководящих указаний.

Совет Европы – Лансаротская конвенция

Конвенция Совета Европы о защите детей от сексуальной эксплуатации и сексуальных злоупотреблений (Лансаротская конвенция) требует от государств принятия комплексных мер по борьбе с сексуальным насилием в отношении детей на основе подхода со следующими элементами: предотвращение, защита, судебное преследование и поощрение национального и международного сотрудничества. Комитет участников Конвенции о защите детей от от сексуальной эксплуатации и сексуальных злоупотреблений ("Комитет Лансароте") уточнил действие Конвенции в отношении цифровой среды, приняв ряд документов. К ним относятся следующие: Мнение о создаваемых, пересылаемых и получаемых детьми изображениях и/или видеоматериалах непристойного или явно сексуального характера с участием детей (6 июня 2019 г.); Мнение о толковании применимости Конвенции Лансароте к сексуальным преступлениям в отношении детей, упрощенным благодаря использованию ИКТ (12 мая 2017 г.); Декларация о веб-адресах, содержащих рекламу материалов или изображений, пропагандирующих сексуальную эксплуатацию детей или любые другие преступления, признанные таковыми в соответствии с Конвенцией Лансароте (16 июня 2016 г.); и Мнение относительно Статьи 23 Конвенции Лансароте – Груминг детей в сексуальных целях с помощью информационно-коммуникационных технологий. Комитет Лансароте осуществляет мониторинг реализации положений Конвенции: его второй тематический раунд мониторинга сосредоточен на защите детей от сексуальной эксплуатации и сексуального насилия при помощи ИКТ: в 2020 году будет опубликован доклад о раунде мониторинга. По состоянию на 2019 год к Конвенции присоединились 46 государств, включая Тунис – первое государство, не являющееся членом Совета Европы.

Иные руководящие принципы Совета Европы

Прочие стандарты и инструменты Совета Европы способствуют выработке коллективного свода правил для создания всеобъемлющих рамок, ориентированных на все заинтересованные стороны. Конвенция Совета Европы о киберпреступности содержит обязательства для участников по введении уголовного преследование за совершение целого ряда преступлений, связанных с материалами, касающимися сексуальных злоупотреблений в отношении детей: в настоящее время ее ратифицировали 64 государства-участника. В частности Совет Европы уделяет особое внимание расширению возможностей детей и их близких безопасно ориентироваться в цифровой сфере. Этому способствуют образовательные инструменты, включая полностью пересмотренный Справочник по вопросам грамотности в интернете (2017 г.), "Руководство по воспитанию цифровой гражданственности" (2019 г.) и пособия, предназначенные для родителей ("Родители в цифровую эпоху"- Руководство для родителей по защите детей от сексуальной эксплуатации и сексуальных злоупотреблений в онлайновой среде (2017 г.); "Цифровое гражданство... и ваш ребенок"- то, что должен знать и делать каждый родитель (2019 г.). Наконец, Совет Европы провел консультативное исследование с детьми в отношении их прав в цифровой среде – "Это наш мир: Взгляды детей на то, как защитить их права в цифровой среде" (2017 г.), и начал проведение консультативных исследований, посвященных опыту детей-инвалидов в цифровой среде – "Два клика вперед и один клик назад: доклад о детях-инвалидах в цифровой среде" (2019 г.).

[44] Council of Europe (2020), The Digital Environment, https://www.coe.int/en/web/children/the-digital-environment. The Council of Europe Guidelines to respect, protect and fulfil the rights of the child in the digital environment is the first such set of standards adopted by an intergovernmental body (CM/Rec, 2018).

Отчет о безопасности ребенка в онлайновой среде

Безопасность ребенка в онлайновой среде: минимизация риска насилия, жестокого обращения и эксплуатации в онлайновой среде, а также Всеобщая декларация безопасности ребенка в онлайновой среде [45].

Рекомендации ОЭСР по защите ребенка в онлайновой среде (2012 г./Пересм. 2019–2020 гг.). Кроме того, следует выделить другие национальные и международные инициативы, способствующие укреплению международного сотрудничества, а также национальных усилий по разработке стратегий защиты ребенка в онлайновой среде, например:

Международная база данных изображений, содержащих элементы сексуальной эксплуатации детей

Международная база данных изображений, содержащих элементы сексуальной эксплуатации детей (БД ICSE), ведется Интерполом и является мощным инструментом получения информации и ведения расследований, который позволяет специализированным следователям обмениваться данными с коллегами по всему миру. БД ICSE, доступ к которой осуществляется через защищенную глобальную коммуникационную систему полиции Интерпола (известную как I-247), использует сложное программное обеспечение для сравнения изображений, чтобы установить связь между жертвами, злоумышленниками и местами. БД ICSE позволяет сертифицированным пользователям в государствах-членах получать доступ к базе данных в режиме реального времени – исследовать существующие элементы, загружать новые данные, сортировать материалы, проводить анализ и общаться с другими экспертами по всему миру по вопросам, связанным с расследованием случаев сексуальной эксплуатации детей.

Глобальный альянс WePROTECT

Глобальный альянс WePROTECT (WPGA) является глобальным движением, в котором объединены влияние, опыт и ресурсы, необходимые для трансформации методов борьбы с сексуальной эксплуатацией детей в онлайновой среде (OSCE) во всем мире. Это союз правительственных структур, глобальных технологических компаний и организаций гражданского общества. Его многосторонний характер уникален в этой области. Видение Глобального альянса WePROTECT заключается в выявлении и защите большего количества жертв, задержании большего количества преступников и прекращении сексуальной эксплуатации детей в онлайновой среде.

Глобальный альянс WeProtect включает ряд компонентов, в частности, модели национальных мер реагирования и глобального стратегического ответа. Более подробная информация содержится в Дополнении 3.

Индекс безопасности ребенка в онлайновой среде 2020 года

Разработанный институтом DQ Индекс безопасности ребенка в онлайновой среде (COSI) 2020 года является первой в мире работающей в режиме реального времени аналитической платформой, помогающей странам отслеживать состояние безопасности детей онлайн.

COSI базируется на шести аспектах, которые образуют рамки COSI. Первый и второй аспекты – киберриски и упорядоченное использование цифровой среды – касаются разумного использования цифровых технологий. Третий и четвертый аспекты – цифровая компетентность и руководящие указания и обучение – связаны с расширением прав и возможностей. Последние два аспекта связаны с инфраструктурой, это аспекты социальной инфраструктуры и установления соединений.

3.3 Примеры реагирования на источники вреда в онлайновой среде

В Дополнении 4 приведен ряд примеров реагирования на источники вреда в онлайновой среде. Эти примеры охватывают ответные меры в области образования, законодательства и выявления вреда в интернете.

[45] Broadband Commission for Sustainable Development (2019), The State of Broadband 2019: Broadband as a Foundation for Sustainable Development, https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf.

3.4 Преимущества национальной стратегии защиты ребенка в онлайновой среде

Гармонизация законодательства

Принятие всеми странами надлежащего законодательства против неправомерного использования ИКТ в преступных или иных целях имеет важнейшее значение для обеспечения глобальной 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[46].

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. Это требует, прежде всего, принятия необходимых положений уголовного законодательства для введения уголовного преследования таких действий, как компьютерное мошенничество, незаконный доступ, вмешательство в данные, нарушение авторских прав, CSAM, а также предотвращения ненадлежащего уголовного преследования детей. 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 – выявление и определение законодательных формулировок и справочных материалов, которые могут помочь странам в разработке согласованных законов и процессуальных норм по проблематике киберпреступности. 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 и соответствующими заинтересованными сторонами и вносит большой вклад в продвижение вперед процесса согласования законодательства по борьбе с киберпреступностью на глобальном уровне.

С учетом быстрых темпов технологических инноваций, в качестве потенциальных решений проблемы устаревания существующей системы регулирования и медленного процесса разработки законодательных норм были выдвинуты концепции саморегулирования и совместного регулирования. Вместе с тем, для того чтобы быть эффективными, регуляторным/директивным органам необходимо четко определить конкретные цели и проблемы в области защиты ребенка в онлайновой среде, реализовать четкий процесс обзора и методологию оценки эффективности саморегулирования и совместного регулирования, а в случае, если в процессе саморегулирования и совместного регулирования не удается решить выявленные проблемы, приступить к официальному процессу разработки законодательства для решения этих проблем. Кроме того, успешные меры саморегулирования могут постепенно переводиться в плоскость формального законодательства в рамках законодательного процесса, с тем чтобы стать правовым предохранителем и не допустить сворачивания или прекращения осуществления некоторых инициатив в области саморегулирования.

Координация

Вполне вероятно, что среди действующих лиц и заинтересованных сторон уже существует целый ряд существующих мероприятий и действий, направленных на защиту ребенка в онлайновой среде, но они имеют спорадический характер. Важно иметь представление о такой деятельности, чтобы учесть уже предпринимаемые усилия при разработке национальной стратегии защиты ребенка в онлайновой среде. Такая стратегия будет координировать и направлять усилия посредством организации как существующих, так и новых видов деятельности.

[46] Комиссия по широкополосной связи в интересах устойчивого развития (2019 г.).

4 Рекомендации по принципам и реализации

Правительства должны бороться со всеми проявлениями насилия в отношении детей в цифровой среде. Однако меры, принимаемые для защиты детей в цифровой среде, не должны необоснованно ограничивать осуществление других прав, таких как право на свободу выражения мнений, право на доступ к информации или право на свободу ассоциаций. Вместо того, чтобы ограничивать естественное любопытство и способность детей к инновации из опасения их столкновения с рисками в онлайновой среде, крайне важно использовать изобретательность детей и повышать их приспособленность в процессе исследования потенциала цифровой среды.

Во многих случаях акты насилия в отношении детей совершаются другими детьми. В таких ситуациях правительства должны, насколько это возможно, применять восстановительные подходы, при которых причиненный вред устраняется, предотвращая при этом уголовное преследование детей. Правительства должны поощрять использование ИКТ в предотвращении насилия и борьбе с ним, например, в разработке технологий и ресурсов, позволяющих детям получать доступ к информации, блокировать вредные материалы и сообщать о случаях насилия в тех случаях, когда они происходят[47].

Чтобы решать проблему глобальной ситуации с безопасностью ребенка онлайн, правительства должны содействовать общению между соответствующими организациями и открыто сотрудничать с целью устранения вреда, причиняемого детям в онлайновой среде.

4.1 Базовые рекомендации

4.1.1 Правовая база

Правительствам следует пересмотреть и, при необходимости, обновить свою правовую базу с целью поддержки полноценной реализации прав ребенка в цифровой среде. Всеобъемлющая правовая база должна касаться превентивных мер; запрещения всех форм насилия в отношении детей в цифровой среде; предоставления эффективных средств реагирования, восстановления и реинтеграции для решения проблем, связанных с нарушениями прав ребенка; создания учитывающих интересы детей механизмов консультирования и сообщения о проблемах и жалобах; а также механизмов подотчетности для борьбы с безнаказанностью[48].

По возможности, законодательство должно быть технологически нейтральным, чтобы его применимость не снижалась в свете будущих технологических разработок[49].

Эффективная реализация законодательных мер требует от правительственных структур дополнительных шагов, включая инициативы по повышению осведомленности и социальной мобилизации, усилия и кампании в области обучения и создания потенциала специалистов, работающих с детьми и в их интересах.

При разработке соответствующего законодательства важно также учитывать, что дети не являются однородной группой. Детям разных возрастных групп могут потребоваться различные ответные меры, равно как и детям с особыми потребностями или детям, которым с большей вероятностью может быть причинен вред в цифровой среде или при ее использовании.

Правительствам следует создать четкую и предсказуемую нормативно-правовую базу, которая помогала бы компаниям и другим третьим сторонам выполнять свои обязанности по защите прав ребенка на протяжении во всех аспектах деятельности, как на территории страны, так и за рубежом[50].

---

47 Special Representative of the Secretary-General on Violence against Children, *Annual Report of the Special Representative of the Secretary-General on Violence against Children to the Human Rights Council,* A/HRC/31/20 (January 2016), para. 103 and 104.

48 Special Representative of the Secretary-General on Violence against Children, *Releasing children's potential and minimizing risks: ICTs, the Internet and Violence against Children,* 2014 (New York: United Nations), p. 55.

49 Special Representative of the Secretary-General on Violence against Children, *Releasing children's potential and minimizing risks: ICTs, the Internet and Violence against Children,* 2014 (New York: United Nations), p. 64.

50 UN Committee on the Rights of the Child, *General Comment № 16*, para. 53.

Директивным органам при исследовании сферы охвата правовых рамок следует принять во внимание приведенные ниже моменты:

- груминг или другие формы дистанционного соблазнения, вымогательства или принуждения детей к неприемлемому сексуальному контакту или сексуальной деятельности;
- владение, производство и распространение CSAM, независимо от намерения распространять;
- домогательства, травля, оскорбления или риторика ненависти в онлайновой среде;
- террористические материалы в онлайновой среде;
- кибербезопасность;
- отражение того факта что то, что является незаконным оффлайн, также является незаконным онлайн.

4.1.2 Политическая и институциональная база

Гарантия реализации прав ребенка в цифровой среде требует от правительств соблюдения баланса между максимизацией преимуществ, получаемых детьми от использования ИКТ, и минимизацией связанных с этим рисков. Этого можно добиться включением мер по защите детей в онлайновой среде в национальные планы по развитию широкополосной сети[51] и разработкой отдельной многосторонней стратегии по защите детей онлайн. Такая повестка дня должна быть полностью интегрирована с любыми существующими политическими принципами, касающимися проблематики прав детей или защиты детей, а также должна дополнять национальную политику в области защиты ребенка, предлагая конкретные основы для всех рисков и потенциальных источников вреда для детей, направленные на создание безопасной, цифровой среды для всех, способствующей расширению прав и возможностей[52].

Правительствам следует создать национальную координационную структуру с четким мандатом и достаточными полномочиями для координации всей деятельности, связанной с правами детей и цифровыми средствами массовой информации и ИКТ, на межсекторальном, национальном, региональном и местном уровнях. Правительства должны сформулировать цели с конкретными сроками их достижения и организовать прозрачный процесс оценки и мониторинга проделанной работы, а также обеспечить выделение необходимых людских, технических и финансовых ресурсов для эффективного функционирования этой структуры[53].

Правительствам следует создать многостороннюю платформу для руководства разработкой, реализацией и мониторингом национальной цифровой повестки дня в интересах детей. Такая платформа должна включать представителей наиболее важных групп населения, включая: детей и молодых людей; ассоциации родителей/опекунов; соответствующие правительственные учреждения; сектор образования, юстиции, здравоохранения и социального обеспечения; национальные правозащитные учреждения и соответствующие регуляторные органы; гражданское общество; компании отрасли; научные круги; и соответствующие ассоциации специалистов.

4.1.3 Нормативная база

Правительственные структуры ответственны за нарушения прав детей, которые стали прямым или косвенным результатом действий компаний, если они не приняли необходимых, надлежащих и разумных мер для предотвращения и исправления таких нарушений или иным образом сотрудничали с такими предприятиями или игнорировали совершаемые ими нарушения[54].

Руководящие принципы предпринимательской деятельности в аспекте прав человека предполагают обеспечение компаниями механизмов правовой защиты и рассмотрения жалоб, которые являются законными, доступными, предсказуемыми, справедливыми, совместимыми с правами, прозрачными, основанными на диалоге и участии, а также могут быть источником постоянного обучения. Механизмы

---

51 The State of the Broadband 2019, Recommendation 5.6, page 78. https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf.

52 For model provisions on child protection for national broadband plans see chapter 10 of the Child Online Safety Report.

53 Special Representative of the Secretary-General on Violence against Children, *Annual Report of the Special Representative of the Secretary-General on Violence against Children* (December 2014) A/HRC/28/55 and *Releasing children's potential and minimizing risks: ICTs, the Internet and Violence against Children,* 2014 (New York: United Nations), para. 88.

54 UN Committee on the Rights of the Child, *General Comment № 16*, para. 28.

рассмотрения жалоб, созданные компаниями, могут обеспечивать гибкие и своевременные альтернативные решения, и их использование при решении проблем, связанных с поведением той или иной компании, может позволить учитывать интересы ребенка. Во всех случаях должен быть обеспечен доступ к судам или судебному пересмотру административных средств защиты и других процедур[55]. Следует рассмотреть механизмы, создающие безопасные, соответствующие возрасту услуги для детей, с тем чтобы пользователи могли сообщать о своих проблемах.

Несмотря на наличие внутренних механизмов рассмотрения жалоб, правительства должны создать механизмы мониторинга для расследования нарушений прав детей и возмещения соответствующего ущерба на предмет повышения подотчетности компаний сферы ИКТ и смежных областей, а также усиления ответственности регуляторных органов за разработку стандартов, относящихся к правам детей и ИКТ[56]. Это особенно важно, поскольку другие средства правовой защиты, имеющиеся в распоряжении пострадавших от действий компаний, такие как гражданский иск и другие средства судебной защиты, зачастую являются сложными и дорогостоящими[57].

Комитет ООН по правам ребенка подчеркнул потенциальную роль национальных правозащитных учреждений в этой области, охарактеризовав роль, которую они могли бы играть в получении и расследовании жалоб на нарушения со стороны отраслевых структур, а также организации посредничества по этим вопросам; проведении государственных расследований крупномасштабных злоупотреблений; проведении пересмотра законодательства с целью обеспечения соблюдения Конвенции о правах ребенка. Комитет указал, что, когда это необходимо, "государствам следует расширить законодательный мандат национальных правозащитных учреждений, с тем чтобы он соответствовал правам детей и интересам бизнеса". Особенно важно, чтобы любой механизм рассмотрения жалоб учитывал интересы детей, обеспечивал неприкосновенность частной жизни и защиту жертв, а также включал деятельность по мониторингу, последующим мерам и проверке в интересах детей-жертв.

Одним из примеров области, в которой национальное правозащитное учреждение или другой регуляторный орган могли бы предоставить детям эффективные средства правовой защиты, является кибертравля. Внутренние механизмы правовой защиты и рассмотрения жалоб порой оказываются неэффективными в таких случаях, поскольку, несмотря на то, что содержание вызывает тревогу и наносит вред, оно часто не рассматривается национальным законодательством, и нет четких оснований для того, чтобы добиваться его удаления структурой, размещающей контент. Наделение государственного органа полномочиями получать жалобы в связи со случаями кибертравли и обращаться к размещающим контент структурам для удаления соответствующих материалов будет являться важным элементом защиты детей[58]. Преимущества такой меры будут заключаться в оперативности реагирования, которая имеет решающее значение в контексте кибертравли, а также в создании четкой правовой основы для решения проблемы удаления материалов, связанных с кибертравлей.

При разработке подхода к регулированию цифровой среды правительства должны также учитывать влияние такого регулирования на осуществление всех прав человека, включая свободу самовыражения[59].

Правительствам следует возложить на предприятия обязательство проявлять должную осмотрительность в вопросах прав ребенка. Это обеспечит работу предприятий по выявлению, предотвращению и смягчению своего воздействия на права детей, в том числе в рамках своих деловых отношений и глобальной деятельности[60].

Кроме того, правительства должны рассмотреть дополнительные меры, такие как обеспечение соблюдения отраслевыми организациями, чья деятельность может оказывать влияние на права детей в цифровой среде, самых высоких стандартов с точки зрения предотвращения возможных нарушений прав и реагирования на них, чтобы иметь право на получение финансирования или заключение контрактов.

---

55 Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, A/HRC/17/31 (2011), para. 71.

56 UN Committee on the Rights of the Child, *Report of the 2014 Day of General Discussion*, para. 96.

57 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/32/38 (2016), para. 71.

58 Bertrand de Crombrugghe, "Report of the Human Rights Council on Its Thirty-First Session" (UN Human Rights Council, 2016).

59 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/32/38 (2016), para. 45.

60 UN Committee on the Rights of the Child, *General Comment № 16*, para. 62.

4.2 Рекомендации практического характера

Правительствам следует обеспечить доступ к эффективным средствам правовой защиты для детей, ставших жертвами нарушения их прав, в том числе помогать им оперативно получить надлежащее возмещение нанесенного ущерба, выплачивая компенсации в случае необходимости. Правительствам следует также оказывать адекватную поддержку и помощь детям, ставшим жертвами нарушений, связанных с цифровыми средствами информации и ИКТ, в частности организовать работу служб комплексной поддержки, для того чтобы обеспечить полное выздоровление и реинтеграцию потерпевших детей, а также предотвратить их повторную виктимизацию[61].

Безопасные и легкодоступные механизмы консультирования, подачи и рассмотрения жалоб, учитывающие интересы детей, такие как телефоны доверия, должны быть предусмотрены законодательно и являться частью национальной системы защиты детей. Важно, чтобы эти службы были связаны с какими-либо регуляторными органами, что помогло бы упростить взаимодействие ребенка с государственными институтами в то время, когда он находится в тяжелом положении. Телефоны доверия особенно ценны с точки зрения очень чувствительных вопросов, таких как сексуальные злоупотребления, которые детям бывает сложно обсудить со сверстниками, родителями, опекунами или учителями. Телефоны доверия также важны, потому что по ним ребенку могут подсказать обратиться, например, в службы юридической помощи, приюты, правоохранительные органы или службы реабилитации[62].

Кроме того, правительства должны понимать и отслеживать поведение правонарушителей, чтобы повысить статистику обнаружения злоумышленников и снизить риск повторного совершения ими правонарушений. Рекомендуется создать телефоны доверия, по которым можно предложить бесплатные и анонимные консультации и поддержку по телефону или в чате потенциальным правонарушителям, у которых возникают чувства или мысли, связанные с сексуальным интересом к детям. Помощь правонарушителям в изменении их поведения сводит к минимуму риск повторного совершения правонарушения.

Установленные на законодательном уровне механизмы рассмотрения жалоб также являются важнейшей частью системы эффективных средств правовой защиты.

Регуляторные органы должны проводить независимые измерения и исследования для оценки того, как платформы сообщают и решают вопросы, связанные с защитой ребенка. Существует технология, позволяющая регуляторным органам самостоятельно проводить мониторинг платформ. Необходимо оказывать помощь поставщикам услуг в целях публикации отчетов, представляемых для обеспечения транспарентности.

Государственные органы вместе с международным сообществом и отраслевыми компаниями должны разработать универсальный набор показателей, которые могли бы использоваться заинтересованными сторонами для измерения всех соответствующих аспектов безопасности ребенка в онлайновой среде.

4.2.1 Сексуальная эксплуатация

Ниже перечислены конкретные соображения, которые следует принять во внимание представителям директивных органов при рассмотрении угроз, способных нанести детям вред, а именно материалов, связанных с сексуальными злоупотреблениями в отношении детей, собственноручно созданного контента, груминга и секс-вымогательства, а также других онлайновых рисков:

- Меры по прекращению или уменьшению трафика передачи материалов CSAM, например, путем создания национальной горячей линии или использования портала IWF для подачи жалоб и блокировки доступа к онлайновому контенту, о котором известно, что он содержит или рекламирует наличие материалов CSAM.
- Обеспечить наличие национальных процедур, что гарантировало бы, что все обнаруженные в стране материалы CSAM будут направляться в централизованный национальный ресурс, который законодательно наделен полномочиями требовать от компаний удаления контента.
- Стратегии контроля спроса на материалы CSAM, в частности для тех, кто уже был признан виновным в совершении таких преступлений. Важно повышать осведомленность о том, что это

[61] UN Committee on the Rights of the Child, *Report of the 2014 Day of General Discussion*, para. 106.
[62] Special Representative of the Secretary-General on Violence against Children, *Releasing children's potential and minimizing risks*, p. 51 and p. 65.

преступление не относится к преступлениям без жертв: дети используются для создания материала, который просматривается, и просматривая и скачивая материалы CSAM по всему миру, каждый непосредственно способствует злоупотреблениям в отношении изображенного там ребенка, а также поощряет использование большего числа детей для создания большего числа изображений.

- Повысить осведомленность о том, что ребенок в принципе не может дать согласие на то, чтобы он подвергался сексуальным злоупотреблениям, для производства материалов CSAM или любым иным способом. Рекомендуйте тем, кто использует материалы CSAM, обратиться за помощью и в то же время информируйте их о том, что они понесут уголовную ответственность за незаконные действия, в которые они вовлечены.
- Другие стратегии контроля спроса на материалы CSAM. Например, в некоторых странах ведется регистр осужденных сексуальных преступников. Суды выписывают юридические предписания, запрещающие таким преступникам либо совсем пользоваться интернетом, 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 определенные веб-сайты или регистрироваться на них, 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, однако объявление такого поведения противозаконным может стать еще одним сдерживающим средством.
- 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 перед травлей или дальнейшей сексуальной эксплуатацией и сексуальными злоупотреблениями. 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.
- 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 и INHOPE. Следует поощрять и использование системы INTERPOL i24/7.
- Обеспечить, чтобы достаточное количество сотрудников органов охраны правопорядка прошли соответствующее обучение по расследованиям преступлений, совершенных в интернете или с использованием компьютеров, а также имели доступ к соответствующим средствам криминалистики, позволяющим им выделять и интерпретировать соответствующие цифровые данные.
- 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.

4.2.2 Образование

В рамках стратегии необходимо обеспечить цифровую грамотность детей, чтобы гарантировать, что они могут получать выгоду от использования технологий, не подвергаясь опасности. Это позволит детям развить навыки критического мышления, которые помогут им определить и понять хорошие и плохие стороны собственного поведения в цифровом пространстве. Важно показать детям пример вреда, который может быть нанесен в онлайновой среде, однако это будет эффективно только в том случае, если это будет сделано в рамках более широкой программы цифровой грамотности, которая должна соответствовать возрасту и фокусироваться на навыках и компетенциях. Важно, чтобы программа обучения безопасности в онлайновой среде включала принципы социального и эмоционального обучения, поскольку они помогут студентам понять эмоции и управлять ими, а следовательно, иметь здоровые отношения на основе уважения как в онлайновой среде, так и в реальном мире.

Один из оптимальных способов обеспечить безопасность детей, пользующихся интернетом, заключается в предоставлении им соответствующих инструментов и знаний. Как вариант, можно включать развитие цифровой грамотности в школьные программы. Другой подход предполагает создание образовательных ресурсов за рамками школьной программы.

Те, кто работает с детьми, должны обладать соответствующими знаниями и навыками, чтобы уверенно помогать детям реагировать на проблемы, связанные с их защитой в онлайновой среде, и решать их, а также обеспечивать приобретение детьми необходимых цифровых навыков для успешного использования технологий.

4.2.3 Отраслевые компании

Национальные и международные отраслевые игроки должны работать над повышением осведомленности о проблемах, связанных с безопасностью ребенка в онлайновой среде, и помогать всем взрослым, ответственным за благополучие ребенка, в том числе родителям и опекунам, школам, молодежным организациям и сообществам, развивать знания и навыки, нужные им для обеспечения безопасности детей. Подход отраслевых компаний к разработке своих продуктов, услуг и платформ должен строиться на принципе повышения безопасности, а обеспечение безопасности должно быть признано основной задачей.

- Предоставить соответствующие возрасту инструменты, учитывающие интересы семьи, чтобы помочь своим пользователям улучшить управление защитой семьи в онлайновой среде.
- Предоставить своим пользователям подходящие механизмы для сообщения о проблемах и вызывающих обеспокоенность вопросах. Пользователи должны ожидать своевременного ответа на эти сообщения с информацией о принятых мерах и, если применимо, о том, где они могут получить дополнительную поддержку.
- Кроме того, обеспечить механизм упреждающего сообщения об эксплуатации детей, чтобы выявить и устранить любые виды злоупотреблений (классифицируемые как преступная деятельность) в отношении детей. Эта практика показала, что если все заинтересованные стороны вносят свой вклад в обнаружение, блокировку и сообщение, то интернет будет более чистым и безопасным для всех. Отраслевые компании должны рассмотреть возможность применения всех соответствующих инструментов, таких как услуги IWF, для предотвращения злонамеренного использования их платформ.

Очень важно, чтобы все соответствующие участники экосистемы знали о рисках и возможностях нанесения вреда в онлайновой среде, чтобы дети не подвергались ненужным рискам.

Необходимо разработать общие показатели безопасности детей в онлайновой среде, чтобы измерить все соответствующие аспекты. Наличие общих стандартов и показателей является единственным способом отслеживания прогресса в странах, определения успешности проектов и мер, нацеленных на искоренение любого насилия в отношении детей, и признания эффективности экосистемы безопасности ребенка в онлайновой среде.

5 Разработка национальной стратегии защиты ребенка в онлайновой среде

5.1 Список для самопроверки на национальном уровне

Для того чтобы сформулировать национальную стратегию, направленную на обеспечение безопасности ребенка в онлайновой среде, директивные органы должны рассмотреть широкий комплекс мер. В Таблице 1 представлены ключевые области, требующие рассмотрения.

Таблица 1: Ключевые области, требующие рассмотрения

	№	Ключевые области, требующие рассмотрения	Дополнительная информация
Правовые рамки	1	Пересмотреть существующие правовые рамки, чтобы установить, что имеются все необходимые юридические права, для того чтобы правоохранительные органы и другие организации защищали людей в возрасте моложе 18 лет в онлайновой среде на всех платформах доступа в интернет.	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.
	2	Установить, *с учетом необходимых изменений*, что любое действие против ребенка, которое является незаконным в реальном мире, является незаконным в онлайновой среде, и что правила защиты данных и конфиденциальности в онлайновой среде применимы также и для детей.	

	№	Ключевые области, требующие рассмотрения	Дополнительная информация
Регуляторные рамки	3	Рассмотреть возможность разработки политики регулирования. Она может предполагать саморегулирование, совместное регулирование, а также полное регулирование. Модель саморегулирования или совместного регулирования может включать разработку и публикацию кодексов добросовестной практики либо базовых ожиданий в плане безопасности в онлайновой среде как в свете оказания содействия привлечению, координации либо организации 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. Модель регулирования может определять ожидания и обязательства заинтересованных сторон и закреплять их в правовом поле. Также могут быть рассмотрены штрафы за несоблюдение политики.	Некоторые страны для разработки правил в этой области создали модель самостоятельного или совместного регулирования, и при помощи таких моделей они, например, публикуют кодексы добросовестной 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. Так, в рамках Европейского союза опубликованы кодексы ЕС, как для сайтов общения в социальных сетях, так и для сетей подвижной телефонной связи, относящиеся к предоставлению контента и услуг детям и молодым людям по этим сетям. Саморегулирование или совместное регулирование может быть более эффективным в плане повышения скорости, с которой могут быть сформулированы и введены в действие соответствующие меры реагирования на технологические изменения. Совсем недавно несколько стран подготовили и/или приняли регуляторные нормы. В этих случаях регуляторные нормы разработаны на основе моделей саморегулирования или совместного регулирования и в них определены требования и ожидания заинтересованных сторон, особенно отраслевых поставщиков, для лучшей защиты своих пользователей.

	№	Ключевые области, требующие рассмотрения	Дополнительная информация
Сообщение о незаконном контенте	4	Обеспечить создание и широкую известность механизма по предоставлению понятных способов сообщать о разнообразном незаконном контенте, обнаруженном в интернете. Например, государственная горячая линия, которая имеет возможность быстрого реагирования и удаления незаконного материала или запрета доступа к нему. Отрасль должна иметь механизмы для выявления, блокировки и устранения злоупотреблений в отношении детей в онлайновой среде с привлечением всех услуг, относящихся к ее организациям.	Механизмы для сообщения о злоупотреблениях при использовании онлайновых услуг или для сообщения о предосудительном или незаконном поведении в онлайновой среде, например по национальной горячей линии, следует широко рекламировать и продвигать как в интернете, так и в других средствах информации. Если национальная горячая линия недоступна, IWF в качестве решения предлагает использовать порталы для направления сообщений. Ссылки на механизмы для сообщения о злоупотреблениях должны быть явно отображены на соответствующих разделах 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 сообщение. 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 скоро присоединятся. См. www.virtualglobaltaskforce.com. См. также INHOPE.
Сообщение о потребностях пользователей	5	Представители отрасли должны предоставить пользователям возможность сообщать о своих вопросах, вызывающих обеспокоенность, и проблемах и реагировать на них соответствующим образом.	На поставщиков следует возложить обязанность предоставлять и ясно указывать своим пользователям возможность сообщать о проблемах и вызывающих обеспокоенность вопросах, касающихся их услуг. Это должно быть удобно и легкодоступно для детей.

	№	Ключевые области, требующие рассмотрения	Дополнительная информация
Участники и заинтересованные стороны	6	Привлечь все соответствующие стороны, заинтересованные в обеспечении защиты ребенка в онлайновой среде, в частности: • правительственные организации; • органы охраны правопорядка; • организации социального обслуживания; • поставщиков услуг интернета и других поставщиков электронных услуг; • поставщиков услуг подвижной телефонии; • поставщиков общественных точек доступа Wi-Fi; • другие соответствующие высокотехнологичные компании; • учительские организации; • родительские организации; • детей и молодых людей; • НПО по защите детей и другие соответствующие НПО; • академические и исследовательские организации; • владельцев интернет-кафе и других поставщиков услуг коллективного доступа, например библиотеки, центры электросвязи, компьютерных клубах[63], центры онлайновых игр и т. д.	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 будет важно понимать, что многие люди повсюду и постоянно подключены к интернету через различные устройства. Должны быть вовлечены операторы широкополосный и подвижной связи и Wi-Fi. Кроме того, во многих странах важным источником доступа в интернет, особенно для детей и молодых людей, является сеть общественных библиотек, центров электросвязи и интернет-кафе.
Исследовательская работа	7	Провести исследование всего спектра национальных участников и заинтересованных сторон для определения их мнений, опыта, вызывающих обеспокоенность вопросов, а также возможностей в том, что касается деятельности по защите ребенка в онлайновой среде. Следует также оценить зону ответственности, а также принимаемые или планируемые меры по защите ребенка в онлайновой среде.	

[63] Компьютерный клуб (англ. "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.

	№	Ключевые области, требующие рассмотрения	Дополнительная информация
Образование: цифровая грамотность и компетентность	8	Разработка материалов по цифровой грамотности в рамках любой национальной школьной программы, которая соответствовала бы возрасту и могла бы применяться для обучения всех детей.	Школы и система образования в целом будут представлять собой основу образования и компонента цифровой грамотности в национальной стратегии защиты детей в онлайновой среде. Любая национальная школьная программа должна включать аспекты защиты детей в онлайновой среде и быть нацелена на то, чтобы дать детям всех возрастов соответствующие их возрасту навыки, чтобы они могли умело и во благо использовать технологии, а также осознавать угрозы и вред, которых следует избегать. В ней должно признаваться и поощряться позитивное и конструктивное поведение в онлайновой среде. В рамках многих образовательных и информационных кампаний важно выбрать правильный тон. Следует избегать пугающих сообщений, и поэтому акцент должен делаться 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. Те, кто работает с детьми, особенно учителя, должны иметь соответствующую подготовку и оснащение, чтобы успешно обучать детей этим навыкам. Они должны понимать, что такое онлайновые угрозы и вред, а также уметь уверенно распознавать признаки злоупотреблений и вреда, реагировать на них и сообщать о своих опасениях, чтобы защищать детей.

	№	Ключевые области, требующие рассмотрения	Дополнительная информация
Образовательные ресурсы	9	Использовать знания и опыт всех заинтересованных сторон и подготовить 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 основным целевым аудиториям. 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 сообщений, отправленных из-за эмоции страха. Пропагандировать положительные и ответственные формы поведения в онлайновой среде. Рассмотреть вопрос о разработке ресурсов, чтобы помогать родителям оценивать безопасность своих детей в онлайновой среде и узнать, как свести к минимуму риски и максимально увеличить потенциал собственной семьи с помощью целенаправленного обучения.	При создании обучающих материалов важно учитывать, что многие люди, мало знающие о технологии, будут чувствовать себя некомфортно, используя ее. По этой причине важно обеспечить, чтобы материалы о безопасности были доступны как в печатном виде, так и в других информационных форматах, которые будут восприниматься новичками как что-то более знакомое, например, видеоролики. 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.
Защита ребенка	10	Гарантировать наличие универсальных системных механизмов защиты ребенка, обязующих все стороны, работающие с детьми (службы социальной защиты, здравоохранения, школы и т. д.), выявлять случаи злоупотреблений и причинения вреда в интернете, реагировать на них и сообщать о таких инцидентах.	Должна существовать универсальная система защиты ребенка, которая применялась бы ко всем, кто работает с детьми, в которой они были бы обязаны сообщать о злоупотреблениях в отношении детей или причинении им вреда, что позволило бы расследовать проблемную ситуацию и найти решение.

	№	Ключевые области, требующие рассмотрения	Дополнительная информация
Осведомленность на национальном уровне	11	Организовать национальные кампании по повышению осведомленности в целях привлечения всеобщего внимания к проблемам защиты ребенка в онлайновой среде. Для разработки кампании может быть полезным использование таких глобальных кампаний, как День более безопасного интернета.	Родители, опекуны и специалисты, такие как учителя, играют важнейшую роль в том, чтобы помогать детям и молодым людям оставаться в безопасности, находясь в сети. Программы поддержки, которые позволят обеспечить осведомленность по этим проблемам, а также определят стратегию борьбы с ними. Следует также рассмотреть вопрос помощи со стороны средств массовой информации в распространении данных и проведении кампаний с целью повышения осведомленности. Такие возможности, как День более безопасного интернета, помогут стимулировать и поощрять обсуждение темы защиты ребенка в онлайновой среде. Многие страны успешно организовали национальные кампании по повышению осведомленности в контексте Дня более безопасного интернета, в которых были задействованы разнообразные участники и заинтересованные стороны, в целях усиления универсального обмена сообщениями в средствах информации и социальных сетях.

	№	Ключевые области, требующие рассмотрения	Дополнительная информация
Инструменты, услуги и настройки	12	Рассмотреть полезную роль, которую способны играть настройки устройств, технические инструменты (например, программы фильтрации) и приложения, обеспечивающие защиту ребенка. Призвать пользователей нести ответственность за свои устройства, регулярно осуществлять обновление операционной системы, а также использовать подходящее программное обеспечение и приложения безопасности.	Существует ряд доступных услуг, которые помогают выявить нежелательные материалы или заблокировать нежелательные контакты. Некоторые из этих программ обеспечения безопасности ребенка и фильтрующих программ могут быть фактически бесплатными, поскольку они являются частью операционной системы компьютера или поставляются как часть пакета услуг поставщиков услуг интернета или поставщиков электронных услуг. Производители некоторых игровых консолей также предоставляют аналогичные инструменты, если устройство допускает выход в интернет. Эти программы не являются гарантией абсолютно надежной защиты, но они могут обеспечить хороший уровень поддержки, особенно в семьях с маленькими детьми. Большинство устройств имеют настройки, помогающие защитить детей, а также способствующие здоровому и сбалансированному использованию. Также существуют механизмы, позволяющие родителям управлять устройствами своих детей с помощью установки времени, выбора приложений и услуг, которые дети могут использовать, и управления покупками. В последнее время были подготовлены отчеты и разработаны настройки, позволяющие пользователям и родителям лучше отслеживать время работы с устройством и доступ к нему и управлять ими. Эти технические инструменты следует использовать как часть более обширного арсенала. Очень важно участие родителей и/или опекунов. Повзрослев, дети потребуют больше конфиденциальности и также ощутят сильное желание начать собственные исследования. Кроме того, там, где между продавцом и потребителем существуют финансовые отношения, очень полезными могут оказаться способы подтверждения возраста, которые помогают продавцам товаров и услуг, имеющих возрастные ограничения, а также издателям материалов, предназначенных только для читателей старше определенного возраста, иметь доступ к этой особой аудитории. Там, где финансовых отношений нет, использование технологий подтверждения возраста может оказаться проблематичным, или во многих странах оно может оказаться невозможным из-за отсутствия

5.2 Примеры вопросов

После определения национальных заинтересованных сторон и участников среди них может быть распространен перечень следующих вопросов с просьбой представить ответы. Их ответы помогут определить область политики, сильные стороны, а также разделы в списке для самопроверки на национальном уровне, на которые следует обратить особое внимание.

- В какой степени вы отвечаете за безопасность детей в онлайновой среде и их права?
- Каким образом безопасность в онлайновой среде и права ребенка интегрированы в ваши существующие политики и процессы?
- В какой степени безопасность в онлайновой среде охватывается действующим законодательством?
- Каковы ваши приоритеты в области безопасности в онлайновой среде?
- Какие виды деятельности вы осуществляете с целью поддержки безопасности в онлайновой среде?
- Имеют ли дети/родители возможность сообщить вам о вызывающих обеспокоенность вопросах или проблемах, касающихся безопасности в онлайновой среде?
- Назовите три основных вызова, стоящих перед вами в онлайновом мире.
- Назовите три главных возможности, открывающихся перед вами в онлайновом мире.

Кроме того, было бы полезно провести исследование, чтобы понять, как дети и их родители представляют себе защиту ребенка в онлайновой среде и каков их опыт.

6 Справочные материалы

Защита ребенка в онлайновой среде: основные документы и публикации

2020 год

- ECPAT International, Sexual Exploitation Of Children In The Middle East And North Africa, 2020
- DQ Institute, 2020 Child Online Safety Report, 2020
- EU Kids Online, EU Kids Online 2020: Survey results from 19 countries, 2020

2019 год

- Internet Watch Foundation (IWF), Annual Report, 2019
- WeProtect Global Alliance, Global Threat Assessment, 2019
- Broadband Commission ITU/UNESCO, Child Online Safety Universal Declaration, 2019
- Broadband Commission ITU/UNESCO, Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online, 2019
- Global Kids Online, Growing up in a connected world, 2019
- Rethinking the Detection of Child Sexual Abuse Imagery on the Internet, in Proceedings of the 2019 World Wide Web Conference, May 13–17, 2019, San Francisco, USA, 2019
- UK Home Office, Online Harms White Paper (UK only), 2019
- PA Consulting, A tangled web: rethinking the approach to online CSEA, 2019
- UK Information Commissioner Office, Consultation on Code of Practice to help protect children online (UK only), 2019
- Global Fund to End Violence against Children, Disrupting Harm: evidence to understand online child sexual exploitation and abuse, 2019
- Global Partnership to End Violence against Children, Safe to Learn Call for Action, Youth Manifesto, 2019

- UNESCO, Behind the numbers: Ending school violence and bullying, 2019 (содержит данные о неприятном поведении и кибертравле в онлайновой среде)
- United Nations Human Rights Office of the High Commissioner, children's rights in relation to the digital environment, 2019
- Australian eSafety Commissioner, Safety by Design Overview, 2019
- UNICEF, Why businesses should invest in digital child safety, 2019
- U.S. Department of State, Trafficking in Persons report, 2019

2018 год

- WeProtect Global Alliance, Global Threat Assessment, 2018
- Child Dignity on the Digital World, Technical Working Group Report, 2018 Council of Europe, Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment, 2018
- Global Fund to End Violence against Children, Two years of supporting solutions: results from the Fund's investments, 2018
- WeProtect Global Alliance, Working examples of Model of National Response capabilities and implementation, 2018
- INTERPOL and ECPAT International, Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material, 2018
- EUROPOL, Internet Organized Crime Threat Assessment (IOCTA), 2018
- NetClean, Report about Child Sexual Abuse Cybercrime, 2018
- International Centre for Missing & Exploited Children (ICMEC), Child Sexual Abuse Material: Model Legislation & Global Review, 9th Edition, 2018
- International Centre for Missing & Exploited Children (ICMEC), Studies in Child Protection: Sexual Extortion and Non-Consensual Pornography, 2018
- International Association of Internet Hotlines, INHOPE Report, 2018
- Internet Watch Foundation (IWF), Annual Report, 2018
- Production and Active Trading of Child Sexual Exploitation Images Depicting Identified Victims
- ITU, Global Cybersecurity Index, 2018
- CSA Centre of Expertise, Interventions for perpetrators of online child sexual exploitation- a scoping review and gap analysis, 2018
- NatCen, Behaviour and Characteristics of Perpetrators of Online-facilitated CSEA - a rapid evidence assessment, 2018
- UNICEF, Policy guide on children and digital connectivity, 2018

2017 год

- The National Center for Missing & Exploited Children (NCMEC), The online enticement of children: an in-depth analysis of CyberTipline Reports, 2017
- Digital Childhood, Addressing Childhood Development Milestones in the Digital Environment
- Childnet, DeShame Report, 2017
- Canadian Centre for Child Protection, Survivors' survey, 2017
- Internet Watch Foundation (IWF), Annual Report, 2017
- International Centre for Missing & Exploited Children (ICMEC), Annual Report, 2017
- International Centre for Missing & Exploited Children (ICMEC), Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review, 2017

- Thorn, Sextortion online survey with 2,097 victims of sextortion ages 13 to 25, 2017
- UNICEF, Children in a Digital World, 2017
- Western Sydney University, Young and Online: Children's Perspectives on Life in Digital Age, 2017
- ECPAT International, Sexual Exploitation of Children in South East Asia, 2017

2016 год

- UNICEF, Perils and possibilities: growing up online, 2016
- UNICEF, Child protection in the digital age: National responses to online CSEA in ASEAN, 2016
- Centre for Justice and Crime Prevention, Child Online Protection in the MENA Region, 2016
- ECPAT International, Interagency Working Group on Sexual Exploitation of Children, Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (The Luxembourg Guidelines), 2016

2015 год

- WeProtect Global Alliance, Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response, 2015
- NCMEC, A Global Landscape of Hotlines Combating CSAM, 2015
- ITU and UNICEF, Guidelines for Industry on Child Online Protection, 2015

О правах человека в цифровом мире

- Council of Europe, Guidelines to respect, protect and fulfil the rights of the child in the digital environment, 2018
- UNESCO, Internet Universality Indicators, 2019
- Ranking Digital Rights (RDR), 2019 RDR Corporate Accountability Index, 2019
- Broadband Commission for Sustainable Development, The State of the Broadband, 2019
- ITU, Measuring Digital Development, 2019
- ITU, Measuring Information Society Report, 2018
- UNICEF, Children and Digital Marketing Industry Toolkit, 2018
- Broadband Commission for Sustainable Development, Digital health, 2017
- Broadband Commission for Sustainable Development, Digital Skills for life and work, 2017
- Broadband Commission for Sustainable Development, Digital gender divide, 2017
- UNICEF, Privacy, protection of personal information and reputation, 2017
- UNICEF, Freedom of expression, association, access to information and participation, 2017
- UNICEF, Access to the Internet and digital literacy, 2017
- Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography

Дополнительные материалы доступны в соответствующем разделе на веб-сайте: www.itu-cop-guidelines.com.

Дополнение 1: Терминология

Приведенные ниже определения опираются главным образом на существующую терминологию, разработанную в рамках Конвенции о правах ребенка 1989 года, а также составленную Межведомственной рабочей группой по сексуальной эксплуатации детей в рамках Руководящих указаний по терминологии в области защиты детей от сексуальной эксплуатации и сексуальных злоупотреблений[64] (Люксембургские руководящие указания, 2016 г.), Конвенции Совета Европы о защите детей от эксплуатации и надругательств сексуального характера 2012 года[65] , а также доклада Global Kids Online 2019 года[66].

Подросток

Подростки – это люди в возрасте от 10 до 19 лет. Важно отметить, что в международном праве отсутствует обязательный термин *подростки* и лица моложе 18 лет рассматриваются как дети, тогда как 19-летние лица считаются взрослыми, кроме случаев, когда совершеннолетие наступает раньше в соответствии с национальным законодательством[67].

Искусственный интеллект (ИИ)

В самом широком смысле данный термин расплывчато определяет системы, относящиеся к области чистой научной фантастики (так называемый "сильный" ИИ, обладающий формой самосознания), и системы, уже действующие и способные выполнять очень сложные задачи (распознавание голоса или лиц, вождение автомобиля: эти системы описываются как "слабый" или "средний" ИИ)[68].

Системы ИИ

Система ИИ – это система на основе машин, которая в рамках заданного набора определенных человеком целей может составлять прогнозы, выносить рекомендации или принимать решения, оказывающие воздействие на реальную или виртуальную среду, и предназначена для функционирования с различным уровнем автономности[69].

Наилучшие интересы ребенка

Описывает все элементы, необходимые для принятия решения в конкретной ситуации для конкретного ребенка или группы детей[70].

---

64 "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse", 2016, 114, http://luxembourgguidelines.org/wp-content/uploads/2017/06/Terminology-guidelines-396922-EN.pdf.

65 Council of Europe, Conseil de l'Europe, and Council of Europe, Protection of Children against Sexual Exploitation and Sexual Abuse: Council of Europe Convention (Strasbourg: Council of Europe Publishing, 2012), https://www.coe.int/t/dg3/children/1in5/Source/Lanzarote%20Convention_EN.pdf.

66 Globalkidsonline.net, "Done Right, Internet Use Can Increase Learning and Skills", November 2019, http://globalkidsonline.net/synthesis-report-2019/.

67 UNICEF and ITU, Guidelines for Industry on Child Online Protection (itu.int/cop, 2015), https://www.itu.int/en/cop/Documents/bD_Broch_INDUSTRY_0909.pdf.

68 Council of Europe, "What's AI?", coe.int, Artificial Intelligence, дата обращения: 16 января 2020 года, https://www.coe.int/en/web/artificial-intelligence/what-is-ai.

69 OECD, "Recommendation of the Council on Artificial Intelligence" (OECD, 2019), https://webcache.googleusercontent.com/search?q=cache:hTtMv9k1ak8J:https://legalinstruments.oecd.org/api/print%3Fids%3D648%26lang%3Den+&cd=3&hl=en&ct=clnk&gl=ch&client=safari.

70 OHCHR, "Convention on the Rights of the Child", дата обращения: 16 января 2020 года, https://www.ohchr.org/en/professionalinterest/pages/crc.aspx.

Ребенок

В соответствии со Статьей 1 Конвенции о правах ребенка, ребенком является любое лицо моложе 18 лет, если национальным законодательством не предусмотрен более ранний возраст совершеннолетия[71].

Сексуальная эксплуатация и сексуальные злоупотребления в отношении детей (CSEA)

Данное понятие описывает все формы сексуальной эксплуатации и сексуальных злоупотреблений (Конвенция о правах ребенка 1989 г., Статья 34), например: "a) склонение или принуждение ребенка к любой незаконной сексуальной деятельности; b) использование в целях эксплуатации детей в проституции или в другой незаконной сексуальной практике; c) использование в целях эксплуатации детей в порнографии и порнографических материалах", а также "половой контакт, как правило с применением силы в отношении лица без его согласия". Сексуальная эксплуатация и сексуальные злоупотребления в отношении детей все чаще происходят с использованием интернета или тем или иным образом связаны с онлайновой средой[72].

Материалы, связанные с сексуальной эксплуатацией и сексуальными злоупотреблениями в отношении детей (CSAM)

Стремительное развитие ИКТ привело к появлению новых форм сексуальной эксплуатации и сексуальных злоупотреблений в отношении детей в онлайновой среде, которые могут совершаться в виртуальной форме и не обязательно подразумевают личную встречу с ребенком[73]. Хотя во многих юридических системах изображения и видеоматериалы, связанные с сексуальными злоупотреблениями в отношении детей, по-прежнему рассматриваются как "детская порнография" или "непристойные изображения детей", в настоящих Руководящих указаниях они будут совокупно именоваться материалами, связанными с сексуальными злоупотреблениями в отношении детей (здесь и далее CSAM). Это соответствует Руководящим указаниям Комиссии по широкополосной связи и модели реагирования на национальном уровне, разработанной Глобальным альянсом WePROTECT[74]. Этот термин более точно описывает данный контент. Порнография подразумевает законное коммерческое производство; в Люксембургских руководящих указаниях дается следующее определение использованию термина "детская порнография": он "*может (произвольно или непроизвольно) способствовать облегчению степени тяжести, уменьшению значимости или даже легитимизации того, что по сути является сексуальными злоупотреблениями в отношении детей и/или их сексуальной эксплуатацией [...]. Термин "детская порнография" создает опасность его толкования таким образом, будто действия совершаются с согласия ребенка и представляют собой законный материал сексуального характера*"[75].

Термин CSAM относится к материалу, представляющему собой деяния, которые являются которые являются сексуальными злоупотреблениями в отношении детей и/или их сексуальной эксплуатацией. Это включает в том числе запись материалов, связанных с сексуальными злоупотреблениями в отношении детей со стороны взрослых; изображения детей, вовлеченных в откровенные сексуальные действия, половых органов детей, в случаях когда изображения делаются или используются в первую очередь для целей сексуального характера.

71 OHCHR; UNICEF and ITU, *Guidelines for Industry on Child Online Protection*.

72 "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse".

73 "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse"; UNICEF, "Global Kids Online Comparative Report (2019)".

74 WePROTECT Global Alliance, "Preventing and Tackling Child Sexual Exploitation and Absue (CSEA): A Model National Response", 2016, https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/582ba50bc534a51764e8a4ec/1479255310190/WePROTECT+Global+Alliance+Model+National+Response+Guidance.pdf; Broadband Commission, "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online (2019)".

75 "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse".

Дети и молодые люди

Означает всех лиц моложе 18 лет, при этом к детям, которые в настоящих руководящих указаниях также именуются детьми младшего возраста, относятся все лица моложе 15 лет, а молодые люди составляют возрастную группу от 15 до 18 лет.

Игрушки, имеющие выход в интернет

Игрушки, имеющие выход в интернет, соединяются с ним при помощи таких технологий как Wi-Fi и Bluetooth и обычно работают в сочетании со специальными приложениями, обеспечивая детям возможность интерактивной игры. Согласно проведенному компанией Juniper Research исследованию, в 2015 году объем рынка игрушек, имеющих выход в интернет, достиг 2,8 млрд. долл. США и, согласно прогнозам, к 2020 году вырастет до 11 млрд. долл. США. Эти игрушки собирают и хранят персональную информацию о детях, в том числе имена, данные геолокации, адреса, фотографии, аудио- и видеозаписи[76].

Кибертравля, также именуемая травлей в онлайновой среде

В международном праве нет определения кибертравли. Для целей настоящего документа под кибертравлей понимается намеренное агрессивное действие, неоднократно осуществляемое группой лиц или отдельным лицом при помощи цифровых технологий и направленное против жертвы, которой трудно защитить себя[77]. Обычно она подразумевает "использование цифровых технологий и интернета для размещения чувствительной информации о ком-либо, намеренное распространение сведений личного характера, нежелательных фотографий или видео, направление сообщений с угрозами или оскорблениями (по электронной почте, в формате мгновенного обмена сообщениями, в чатах и текстовых сообщениях), распространение сплетен и ложной информации о жертве или намеренное исключение ее из онлайнового общения"[78]. Она может происходить напрямую (в чатах или текстовых сообщениях), в рамках сообщества с ограниченным доступом (рассылка постов и раздражающих сообщений по списку электронных адресов) или же в общественном доступе (например, создание сайтов специально для издевательства над жертвами).

Киберненависть, дискриминация и насильственный экстремизм

"Киберненависть, дискриминация и насильственный экстремизм представляют собой отчетливую форму кибернасилия, которая направлена против коллективной идентичности, а не против отдельных людей [...] и нередко затрагивает расу, сексуальную ориентацию, религию, национальность или иммиграционный статус, половую/гендерную принадлежность и политический аспект"[79].

Цифровое гражданство

Цифровое гражданство означает осуществление полезной, ответственной и компетентной деятельности в цифровой среде с применением навыков эффективной коммуникации и творческого подхода для воплощения форм социального участия, основанных на уважении прав человека и человеческого достоинства, путем ответственного использования технологий[80].

---

76 Jeremy Greenberg, "Dangerous Games: Connected Toys, COPPA, and Bad Security", Georgetown Law Technology Review, December 4, 2017, https://georgetownlawtechreview.org/dangerous-games-connected-toys-coppa-and-bad-security/GLTR-12-2017/.

77 Anna Costanza Baldry, Anna Sorrentino, and David P. Farrington, "Cyberbullying and Cybervictimization versus Parental Supervision, Monitoring and Control of Adolescents' Online Activities", Children and Youth Services Review 96 (January 2019): 302–7, https://doi.org/10.1016/j.childyouth.2018.11.058.

78 UNICEF, "Global Kids Online Comparative Report (2019)"; "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse".

79 UNICEF, "Global Kids Online Comparative Report (2019)".

80 Council of Europe, "Digital Citizenship and Digital Citizenship Education", Digital Citizenship Education, дата обращения: 16 января 2020 года, https://www.coe.int/en/web/digital-citizenship-education/home.

Цифровая грамотность

Цифровая грамотность означает наличие навыков, необходимых для жизни, обучения и работы в обществе, где коммуникации и доступ к информации все больше обеспечиваются за счет использования цифровых технологий, таких как интернет-платформы, социальные сети и мобильные устройства[81]. Она включает в себя непосредственно коммуникации, технические навыки и критическое мышление.

Устойчивость к воздействию цифровой среды

Данный термин описывает способность ребенка эмоционально справиться с вредоносными факторами в онлайновой среде. Устойчивость к воздействию цифровой среды подразумевает наличие эмоциональных ресурсов, необходимых для того, чтобы понимать, когда ребенок подвергается риску в интернете, знать, как обращаться за помощью, извлекать практические уроки и восстанавливаться после неудачного опыта[82].

Педагоги

Педагог – это лицо, ведущее систематическую работу по усовершенствованию знаний другого лица по данному предмету. Роль педагога предполагает как работу в школе, так и более неформальную педагогическую деятельность, например такую, когда для предоставления информации о безопасности в онлайновой среде или проведения учебных курсов на базе общины или школы для того, чтобы дети и молодые люди были в безопасности в онлайновой среде, используются платформы сайтов социальных сетей.

Работа педагога может варьироваться в зависимости от условий его деятельности и возрастной группы детей и молодых людей (или взрослых), на обучение которых направлены его усилия.

Груминг/груминг в онлайновой среде

Груминг/груминг в онлайновой среде, согласно Люксембургским руководящим указаниям, означает процесс налаживания/построения взаимоотношений с ребенком лично или при помощи интернета или других цифровых технологий с целью добиться сексуальных связей с этим лицом в онлайновой среде или в реальной жизни, склонив ребенка вступить в сексуальную связь[83]. Процесс, направленный на завлекание детей в действия или беседы сексуального характера, как с их ведома, так и без него, или процесс, предполагающий общение и установление отношений между нарушителем и ребенком с целью сделать последнего более уязвимым перед сексуальными злоупотреблениями. Термин "груминг" не закреплен в международном праве; в некоторых юридических системах, в том числе в Канаде, используется термин "завлекание".

Информационно-коммуникационные технологии (ИКТ)

Информационно-коммуникационные технологии означают все информационные технологии, в которых основной акцент приходится на коммуникацию. К ним относятся все использующие подключение к интернету услуги и устройства, такие как компьютеры, ноутбуки, планшеты, смартфоны, игровые приставки, телевизоры и часы[84], а также другие. Сюда же относятся услуги, например радио, широкополосная связь, сетевое оборудование и спутниковые системы.

---

81 Western Sydney University-Claire Urbach, "What Is Digital Literacy?", дата обращения: 16 января 2020 года, https://www.westernsydney.edu.au/studysmart/home/digital_literacy/what_is_digital_literacy.

82 Dr. Andrew K. Przybylski, et al., "A Shared Responsibility. Building Children's' Online Resilience Report" (ParentZone, University of Oxford and Virgin Media, 2014), https://parentzone.org.uk/sites/default/files/Building%20Online%20Resilience%20Report.pdf.

83 "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse".

84 UNICEF and ITU, *Guidelines for Industry on Child Online Protection.*

Интернет и связанные с ним технологии

Теперь можно подключаться к интернету, используя различные устройства, например смартфоны, планшеты, игровые приставки, телевизоры и ноутбуки, а также обычные компьютеры. Таким образом, за исключением случаев, когда контекст предполагает иное, следует понимать, что любая ссылка на интернет охватывает все это разнообразие способов подключения. Чтобы отобразить богатство и сложность интернета, выражения "интернет и связанные с ним технологии", "ИКТ и онлайновая индустрия" и "интернет-услуги" используются взаимозаменяемо.

Уведомление и удаление

Операторы и поставщики услуг иногда получают уведомления о подозрительном контенте в интернете от потребителей, представителей общественности, правоохранительных органов или организаций горячей линии. Процедуры уведомления и удаления – предпринимаемые компанией действия по быстрому удалению ("удаление") незаконного контента (незаконный контент определяется согласно законодательству), как только компании становится известно о наличии такового в ее услугах ("уведомление").

Онлайновые игры

Термин "онлайновые игры" означает участие в платных цифровых играх любого вида с участием одного или многих игроков с использованием любого устройства, имеющего выход в интернет, в том числе специальных приставок, стационарных компьютеров, ноутбуков, планшетов и мобильных телефонов.

"Экосистема онлайновых игр", согласно своему определению, включает в себя наблюдение за процессом видеоигр других людей с использованием платформ электронного спорта, потокового видео или обмена видеоматериалами, которые обычно предусматривают для зрителей возможность оставлять комментарии или общаться с игроками и другими представителями аудитории[85].

Инструменты родительского контроля

Программное обеспечение, которое позволяет пользователям (как правило, родителям) контролировать некоторые или все функции компьютера или иного устройства, способного поддерживать связь с интернетом. Обычно такие программы позволяют ограничивать интернет-доступ к определенным видам или категориям вебсайтов или онлайновых услуг. Некоторые также имеют настройки времени, то есть устройство можно настроить таким образом, чтобы оно подключалось к интернету только в определенные промежутки времени. Более совершенные версии позволяют вести запись всех отправляемых или получаемых при помощи устройства текстовых сообщений. Как правило, такие программы защищаются паролями[86].

Родители и опекуны

На ряде сайтов в интернете присутствует обобщенное упоминание родителей (как, например, на "родительской странице" или упоминание "родительского контроля"). Поэтому было бы целесообразно определить тех людей, которые будут наилучшим образом предоставлять детям возможности максимального использования возможностей интернета, обеспечивая при этом безопасное и ответственное использование интернет-сайтов детьми и молодыми людьми, а также давать им свое согласие на получение доступа к конкретным интернет-сайтам. В настоящем документе термин "родители" означает любое лицо (кроме педагога), которое несет юридическую ответственность за ребенка. Степень ответственности родителей, а также юридические родительские права являются разными в различных странах.

---

[85] UNICEF, "Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry", DISCUSSION PAPER SERIES: Children's Rights and Business in a Digital World, 2019, https://www.unicef-irc.org/files/upload/documents/UNICEF_CRBDigitalWorldSeriesOnline_Gaming.pdf.

[86] UNICEF and ITU, *Guidelines for Industry on Child Online Protection.*

Персональная информация

Термин означает индивидуально определяемую информацию о лице, которая собирается в онлайновом режиме. К ней относятся полное имя, контактная информация, такая как домашний адрес и адрес электронной почты, номера телефонов, отпечатки пальцев или данные для распознавания лиц, номера страховок или любые другие сведения, позволяющие вступить в физический или виртуальный контакт или определить местоположение лица. В этом контексте персональная информация также означает любую информацию о ребенке и его окружении, которая собирается в онлайновом режиме поставщиками услуг интернета, включая игрушки с выходом в интернет и интернет вещей, а также любые другие технологии, использующие соединение с интернетом.

Конфиденциальность

Конфиденциальность нередко оценивается с точки зрения распространения персональной информации в онлайновой среде, наличия открытого профиля в социальных сетях, обмена информацией с незнакомыми людьми в интернете, использования настроек конфиденциальности, предоставления паролей друзьям, осознанием важности сохранения конфиденциальности[87].

Секстинг

Секстинг обычно определяется как отправка, получение собственноручно созданного сексуального контента, включая изображения, сообщения или видео, или обмен им при помощи мобильных телефонов и/или интернета[88]. В большинстве стран создание, распространение и хранение изображений детей сексуального характера является незаконным. В случае распространения изображений детей сексуального характера взрослые не должны просматривать их. Демонстрация изображений сексуального характера ребенку взрослым всегда представляет собой преступное деяние; распространение таких изображений между детьми может нанести вред; следует сообщать о подобных инцидентах; может потребоваться помощь по устранению распространенных изображений.

Секс-вымогательство, или сексуальное вымогательство в отношении детей

Секс-вымогательство, или сексуальное вымогательство (также называемое "сексуальным принуждением или вымогательством в онлайновой среде")[89] означает "шантаж лица при помощи собственноручно созданных изображений этого лица в целях вымогания у него сексуальных услуг, денег или других благ под угрозой распространения материала без согласия фигурирующего в нем лица (например, при помощи размещения изображений в социальных сетях)"[90].

Интернет вещей (IoT)

Интернет вещей является следующим шагом в направлении цифровизации общества и экономики, когда взаимосвязь людей и объектов осуществляется через коммуникационные сети, а также передаются сведения об их состоянии и окружающей обстановке[91].

87 "Children's Online Privacy Protection Act", Pub. L. No. 15 U.S.C. 6501-6505 (1998), https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim.

88 "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse".

89 Europol, "Online Sexual Coercion and Extortion as a Form of Crime Affecting Children: Law Enforcement Perspective" (European Cybercrime Centre, May 2017), https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf.

90 "Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse".

91 Ntantko, The Internet of Things, 1 October 2013, Digital Single Market – European Commission, https://ec.europa.eu/digital-single-market/en/internet-of-things.

URL

Сокращение от английского "uniform resource locator", т. е. "универсальный указатель ресурса" – адрес страницы в интернете [92].

Виртуальная реальность

Виртуальная реальность – это создание при помощи компьютерных технологий эффекта трехмерного мира, в котором объекты воспринимаются как реально существующие в пространстве[93].

Wi-Fi

Wi-Fi (от англ. "Wireless Fidelity" – "высокая точность беспроводной передачи") – набор технических стандартов, обеспечивающих возможность передачи данных по беспроводным сетям [94].

92 UNICEF and ITU, *Guidelines for Industry on Child Online Protection.*
93 NASA, "Virtual Reality", nas.nasa.gov, дата обращения: 16 января 2020 года, https://www.nas.nasa.gov/Software/VWT/vr.html.
94 Children's Online Privacy Protection Act.

Дополнение 2: 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 из этих контактов могут иметь сексуальную природу.

Согласно исследованиям, 22% подвергались травле[95], домогательствам или преследованию в сети; 24% получали нежелательные сексуальные комментарии[96]; 8% встречались в реальной жизни с людьми, с которыми до этого общались только в сети[97]. Хотя значения для разных стран и разных регионов разные, эти цифры показывают, что риски являются реальными[98]. В одном исследовании интернета, проведенном в Соединенных Штатах Америки[99], отмечено, что 32% подростков общались с совершенно незнакомым человеком, 23% из них сказали, что им было страшно и неудобно во время беседы; и 4% подвергались настойчивым и агрессивным сексуальным приставаниям.

Сексуальные интернет-хищники используют интернет для общения с детьми и молодыми людьми с сексуальными целями, часто пользуясь приемами, известными 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. Для преследования и соблазнения ребенка или молодого человека используются подарки, деньги, даже билеты на транспорт, чтобы завлечь его туда, где интернет-хищник сможет совершить сексуальное насилие над ним или ней. Может даже производиться фото- или видеосъемка этих встреч. Детям и молодым людям часто не хватает эмоциональной зрелости и чувства собственного достоинства, что делает их уязвимыми для манипуляций и травли. Они также боятся сказать взрослым о своих встречах, опасаясь попасть в неловкое положение или потерять доступ к интернету. В некоторых случаях они затравлены интернет-хищниками и им приказано держать эту связь в тайне. Кроме того, сексуальные интернет-хищники учатся друг у друга в интернет-форумах и чатах.

95 U-report (2019), http://www.ureport.in/v2/.

96 Project deSHAME (2017), https://www.childnet.com/ufiles/Project_deSHAME_Dec_2017_Report.pdf.

97 Lenhardt, A., Anderson, M., Smith, A. (2015), Teens, Technology and Romantic Relationships, https://www.pewresearch.org/internet/2015/10/01/teens-technology-and-romantic-relationships/.

98 Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011). *Risks and safety on the internet: The perspective of European children. Full findings*. LSE, London: EU Kids Online, http://eprints.lse.ac.uk/33731/.

99 Amanda Lenhart et al., "The Use of Social Media Gains a Greater Foothold in Teen Life as They Embrace the Conversational Nature of Interactive Online Media", *Pew Internet and American Life Project*, 2007, 44, https://www.pewinternet.org/wp-content/uploads/sites/9/media/Files/Reports/2007/PIP_Teens_Social_Media_Final.pdf.pdf.

Дополнение 3: Глобальный альянс WeProtect

Модель типовых национальных мер реагирования WePROTECT

Стратегия Глобального альянса WePROTECT помогает странам разработать скоординированные многосторонние меры реагирования для борьбы с сексуальной эксплуатацией ребенка в онлайновой среде, руководствуясь соответствующей Моделью типовых национальных мер реагирования. Модель типовых национальных мер реагирования Глобального альянса WeProtect выступает в качестве программы мер, которые должны приниматься на национальном уровне. Она предоставляет странам фундамент для борьбы с сексуальной эксплуатацией ребенка в онлайновой среде. Эта Модель типовых национальных мер реагирования предназначена для того, чтобы помочь стране:

- оценить актуальные в настоящее время меры реагирования на проблему сексуальной эксплуатации ребенка в онлайновой среде и выявить пробелы;
- определить приоритетность национальных усилий по заполнению пробелов;
- укрепить понимание и сотрудничество на международном уровне.

Модель не предполагает обязательного характера определенных действий и не предусматривает только один подход. Цель модели – описать возможности, необходимые для эффективной защиты детей, и поддержать страны в развитии или расширении существующих возможностей. В ней также содержится перечень стимулирующих факторов, которые в случае их внедрения и эффективности ускорят достижение результатов и улучшат их. Модель включает двадцать одну возможность, которые сгруппированы в шесть блоков: политика и управление, уголовная юстиция, пострадавшие, социальные вопросы, отрасль, а также средства информации и коммуникации. По мнению Глобального альянса WePROTECT, принятие мер во всех шести блоках обеспечит всестороннее национальное реагирование на такого рода преступления.

Эта модель позволит стране, независимо от текущего состояния дел, выявить любые пробелы в сфере возможностей и начать планирование с целью устранения этих пробелов. Страны будут разрабатывать собственные индивидуальные подходы, однако делая это в контексте единых согласованных рамок и понимания возможностей, можно продолжать развитие связей и сотрудничество между заинтересованными сторонами как на национальном, так и на международном уровнях.

Глобальные стратегические меры реагирования WePROTECT

Глобальные стратегические меры реагирования Глобального альянса WePROTECT – это скоординированный подход к борьбе с сексуальной эксплуатацией ребенка в онлайновой среде, который включает более глубокое осмысление глобальных проблем, международную гармонизацию национальных подходов и глобальные решения в дополнение к национальным мерам реагирования. Глобальные стратегические меры реагирования по сути являются сопутствующим компонентом Модели типовых национальных мер реагирования; в то время как Модель типовых национальных мер реагирования сосредоточена на возможностях, необходимых для решения проблемы сексуальной эксплуатации ребенка в онлайновой среде на национальном уровне, Глобальные стратегические меры реагирования сосредоточены на приоритетных областях международного сотрудничества и создания потенциала.

Глобальные стратегические меры реагирования включают шесть тематических областей, каждая из которых характеризуется необходимыми возможностями и ожидаемыми результатами, а также наличием партнеров, которые для их достижения должны вести совместную работу в разных странах.

Политика и законодательство

Развитие как политической воли к действию, так и законодательства для эффективного согласования подхода к уголовным преступлениям приведет к возобновлению на национальном и международном уровнях обязательств высокого уровня по борьбе с сексуальной эксплуатацией ребенка в онлайновой среде.

Уголовная юстиция

Обмен информацией, в том числе совместный доступ к международным базам данных через официальные структуры обмена данными в сочетании со специализированными, обученными сотрудниками и прокурорами, имеющими опыт работы с сексуальной эксплуатацией ребенка в онлайновой среде, является лучшим способом выявления, преследования и задержания правонарушителей, в том числе благодаря успешному проведению совместных расследований и вынесению приговоров.

Подача заявления пострадавшими, службы оказания помощи

Эффективная и своевременная поддержка жертв, в том числе защита их собственной идентичности и возможность сказать о случившемся, помогает гарантировать жертвам доступ к необходимой поддержке, когда она им нужна.

Технология

Использование технических решений, в том числе искусственного интеллекта, для обнаружения, блокировки и предотвращения распространения материалов вредного содержания, потокового вещания и онлайнового груминга, что требует обязательной и последовательной вовлеченности большого числа представителей технологического сектора, сделает невозможным использование платформ в качестве инструмента для сексуальной эксплуатации ребенка в онлайновой среде.

Социальные вопросы

Существует целый ряд мер, принимаемых обществом в целом, которые в своей совокупности могут дать детям возможность защитить себя от сексуальной эксплуатации в онлайновой среде, где бы они ни жили. Обеспечение безопасности цифровой культуры на уровне проекта (когда функции безопасности встроены) и соблюдение этического и последовательного подхода к освещению в средствах информации ограничат доступ к незаконному контенту в онлайновой среде. При этом образование и информационно-пропагандистская деятельность, ориентированная на детей и родителей, опекунов и специалистов, а также точечные меры в отношении правонарушителей – все это имеет целью предотвращение случаев сексуальной эксплуатации ребенка в онлайновой среде или смягчение их последствий.

Исследование и понимание вопроса

Наконец, оценка угроз (например, Global Threat Assessment 2019) и исследования, посвященные правонарушителям и касающиеся долгосрочных травм жертв, – все это обеспечит правительству, правоохранительным органам, гражданскому обществу, академическим кругам и промышленности четкое понимание актуальных угроз.

Дополнение 4: Меры реагирования на источники вреда в онлайновой среде (примеры)

Сборник приведенных здесь примеров составлен авторами вкладов и авторами руководящих указаний МСЭ для директивных органов.

Разъяснительная работа с детьми, касающаяся источников вреда в онлайновой среде

Приложение Own It компании BBC – приложение для обеспечения благополучия детей в возрасте 8–13 лет, получивших первый смартфон. В этом приложении сочетаются передовые технологии машинного обучения для отслеживания действий детей на их смартфонах и возможность детей самостоятельно сообщить о своем эмоциональном состоянии, при этом эта информация используется для предоставления **адаптированного** контента и принятия мер, что помогает детям оставаться счастливыми и здоровыми в онлайновой среде.

Благодаря наличию специального тематического контента, подготавливаемого в рамках всей компании BBC, приложение делает доступными полезные материалы и ресурсы, что помогает молодым людям максимально эффективно использовать время в онлайновой среде и формировать здоровое поведение и здоровые привычки в онлайновой среде, а также способствует тому, чтобы молодые люди и родители вели более конструктивные беседы о собственном онлайновом опыте. Приложение не собирает ни персональные данные, ни сгенерированный пользователем контент, потому что все машинное обучение происходит в приложении/на устройстве пользователя.

Project Evolve – библиотека обучения цифровым компетенциям, которая полностью обеспечена соответствующими ресурсами и содержит описание цифровых навыков детей всех возрастов; эти материалы помогают родителям и учителям осмыслить компетенции, которые должны иметь дети; имеются также материалы и задания для развития определенных навыков.

360 degree safe – онлайновый инструмент самоконтроля для школ, который дает возможность рассмотреть и дать всестороннюю оценку своей безопасности в онлайновой среде, а также обеспечивает руководство и оказывает поддержку в разработке четких стандартов.

Институт DQ: За 2017–2019 годы в 30 странах мира были собраны данные 145 426 детей и подростков в рамках продвигаемого институтом DQ движения #DQEveryChild – глобального движения за цифровое гражданство, которое началось в Сингапуре при поддержке компании Singtel и быстро разрослось благодаря сотрудничеству со Всемирным экономическим форумом, охватив более 100 партнерских организаций. Это движение было направлено на то, чтобы дети обладали широкими знаниями в области цифрового гражданства с самого начала своей цифровой жизни с помощью онлайновой программы образования и оценки DQ World. Данные этого движения были использованы для создания Индекса безопасности ребенка в онлайновой среде в 2020 году. В Индексе произведена оценка и ранжирование безопасности ребенка в онлайновой среде в 30 странах с использованием 24 факторов влияния на безопасность ребенка в онлайновой среде, сгруппированных в шесть блоков.

Пакет DQ Pro Family Readiness и онлайновая программа DQ World предоставляют родителям возможность оценить цифровую готовность своего ребенка и с использованием учебных материалов улучшить цифровые компетенции, такие как цифровое гражданство, управление временем, проведенным за экраном, борьба с кибертравлей, управление кибербезопасностью, цифровое сопереживание, управление цифровым следом, критическое мышление и управление конфиденциальностью.

Австралийский Комплект инструментов электронной безопасности для школ – это набор ресурсов для поддержки школ в создании более безопасной онлайновой среды. Комплект инструментов отражает многогранный подход к обучению онлайновой безопасности и состоит из четырех блоков с ресурсами, которые:

- готовят школы к оценке их готовности решать вопросы онлайновой безопасности и содержат предложения по улучшению текущей практики;
- привлекают все школьное сообщество к участию в создании безопасной онлайновой среды;
- служат для обучения на базе примеров передового опыта обучения онлайновой безопасности, помогая школам развивать возможности школьной общественности в области безопасности в онлайновой среде;

- позволяют эффективно реагировать на инциденты, сохраняя безопасность и благополучие.

Образовательная кампания I Click Sensibly Управления электронных средств связи (UKE) Польши рассказывает детям и их родителям о том, как повысить онлайновую безопасность и как распознать риски и управлять ими.

ChildFund Вьетнама выступил с инициативой Swipe Safe. В этой программе детям рассказывается о потенциальных рисках в онлайновой среде, таких как кибермошенничество, травля или сексуальные злоупотребления, и даются советы о том, как оставаться в безопасности.

Доклад Комиссии по широкополосной связи, *Технологии, широкополосная связь и образование: ускоренное выполнение программы "Образование для всех"*, 2013 г.

Исследование на тему "Опыт детей в онлайновой среде: обеспечение взаимопонимания и принятие мер на глобальном уровне", ЮНИСЕФ, 2019 г.

Исследовательский проект Global Kids Online содержит обширную информацию о передовой практике реагирования на разные виды онлайнового вреда.

Примеры привлечения отраслевых компаний

Комиссариат по электронной безопасности Австралии выстраивает прочные партнерские отношения и сотрудничает с отраслевыми компаниями, чтобы опыт всех австралийцев в онлайновой среде был более безопасным и позитивным. Примером может служить его инициатива "Безопасность на этапе проектирования". В рамках этой инициативы Комиссариатом по электронной безопасности были проведены подробные консультации с отраслевыми компаниями, торговыми органами и организациями, отвечающими за защиту пользователей, а также родителями, опекунами и молодыми людьми. Инициатива "Безопасность на этапе проектирования" имеет целью поощрять отраслевые компании и помогать им в обеспечении безопасности пользователей начиная с этапов проектирования, разработки и развертывании онлайновых услуг и платформ. Комиссариат по электронной безопасности также администрирует три программы направления сообщений и подачи жалоб: программу в отношении кибертравли, программу в отношении злоупотреблений с использованием изображений и программу в отношении онлайнового контента. Комиссариат по электронной безопасности может официально предписывать определенным поставщикам онлайновых услуг удалять контент. Несмотря на то, что программы в значительной степени действуют как модель сотрудничества между правительством и компаниями отрасли, имеющиеся у Комиссариата по электронной безопасности полномочия по удалению материалов обеспечивают критическую сеть безопасности и побуждают компании отрасли быть инициативными в борьбе с вредом в онлайновой среде.

Компания Telia обязалась проанализировать негативные последствия, связанные подключением, и обеспечить управление ими, а также добиться полной прозрачности и подотчетности на уровне Совета директоров. Компания также проявляет заботу о детях и молодежи, признавая их активными пользователями услуг компании.

Управление электронных средств связи (UKE) Польши привлекает гражданское общество и детей к участию в информационно-пропагандистских кампаниях, чтобы те понимали, под какими документами в онлайновой среде они ставят подпись.

Internet Watch Foundation (Фонд наблюдения за интернетом) – это партнерская организация, объединяющая отраслевые компании, государственные структуры, правоохранительные органы и НПО с целью искоренения практики сексуальных злоупотреблений в отношении детей. В 2020 году в состав IWF входит 152 члена из числа платформ и инфраструктурных служб; членам предлагается ряд услуг по предотвращению распространения криминальных изображений на своих платформах.

Законодательное регулирование

Выразите политическую волю, чтобы придать приоритетное значение защите ребенка в онлайновой среде, – подпишите Всеобщую декларацию о безопасности ребенка в онлайновой среде (Комиссия по широкополосной связи).

Регулирование

Отчет Out of the Shadows: shining light on the response to child sexual abuse and exploitation ("Выйти из тени: освещая меры против сексуальных злоупотреблений в отношении детей и их сексуальной эксплуатации") (Economist Intelligence Unit, 2019) – единственный инструмент, в котором прописаны контрольные показатели реагирования стран на сексуальные злоупотребления в отношении детей и их сексуальную эксплуатацию, включая цифровое пространство, и меры реагирования, принимаемые компаниями ИКТ.

Выявление злоупотреблений в отношении детей в онлайновой среде

Ниже приведены примеры надлежащей практики выявления случаев злоупотреблений в отношении детей в онлайновой среде.

INHOPE: Сеть INHOPE была создана в 1999 году для борьбы с материалами CSAM в онлайновой среде в ответ на единое видение интернета как пространства, свободного от материалов, связанных с сексуальными злоупотреблениями в отношении детьми. За прошедшие 20 лет сеть INHOPE выросла, успешно борясь с увеличением количества материалов CSAM в сети, их географической распространенностью и жестокостью. Сегодня горячие линии INHOPE работают на местах на всех континентах, получают сообщения и незамедлительно удаляют материалы CSAM из интернета, а также обмениваются информацией с правоохранительными органами.

Microsoft PhotoDNA создает хэши изображений и сравнивает их с базой данных хэшей, которые уже определены и подтверждены как материалы CSAM. В случае обнаружения совпадения изображение блокируется. Но этот инструмент не использует технологию распознавания лиц и не может идентифицировать человека либо объект на изображении. Все изменилось с изобретением PhotoDNA for Video.

PhotoDNA for Video разбивает видео на ключевые кадры и фактически создает хэши для этих снимков экрана. Так же, как PhotoDNA может определить изображение, которое было изменено, чтобы избежать обнаружения, PhotoDNA for Video может найти контент с сексуальной эксплуатацией детей, отредактированный или включенный в видео, которое в ином случае было бы безобидным.

Компания Microsoft выпустила новый инструмент для выявления охотящихся на детей интернет-хищников, которые входят в доверие к детям в онлайновых чатах. **Project Artemis**, разработанный в сотрудничестве с The Meet Group, Roblox, Kik и Thorn, выстроен на запатентованной технологии Microsoft и будет свободно распространяться организацией Thorn среди оказывающих онлайновые услуги компаний, предлагающих функцию чата. Project Artemis – это технический инструмент, помогающий предупредить администраторов о необходимости какого-либо модерирования чатов. Эта техника выявления груминга сможет обнаружить интернет-хищников, предпринимающих попытки соблазнения детей в сексуальных целях, принять меры в их отношении и сообщить о них.

Неправительственная организация **Thorn** разработала рекламные объявления, имеющие целью удержать человека от поиска материалов, связанных с сексуальными злоупотреблениями в отношении детей; в течение трех лет эти объявления были размещены в четырех поисковых системах миллионы раз. Так, в объявлениях отмечен 3-процентный рейтинг кликов от людей, обращающихся за помощью после поиска материала, связанного с эксплуатацией.

Thorn's Safer – инструмент, который можно развернуть непосредственно на платформе частной компании для определения и удаления материалов CSAM, а также представления сообщений о таких материалах.

Thorn Spotlight – программное обеспечение, которое дает правоохранительным органам во всех 50 штатах Соединенных Штатов Америки и в Канаде возможность ускорить идентификацию жертв и сократить время расследования более чем на 60%.

На сайте объявлений **Geebo**, администраторы которого приняли на себя обязательство не допускать сексуальной эксплуатации на этой платформе, никогда не было случаев сексуальной эксплуатации детей. Им удается сделать это отчасти благодаря наличию процедуры предварительной проверки.

Классификатор Google AI можно использовать для обнаружения материалов, связанных с сексуальными злоупотреблениями в отношении детей, в сетях, сервисах и на платформах. Этот инструмент доступен бесплатно через **API безопасности контента Google**, пакет программ, расширяющий возможности просмотра контента с участием меньшего числа людей. Этот инструмент поможет экспертам-людям просматривать материалы в еще большем объеме и не отставать от правонарушителей, ориентируясь на

изображения, которые ранее не были помечены как незаконные материалы. Совместное использование этой технологии ускорит идентификацию изображений.

В 2015 году Google расширил свою работу с хэшами, представив первую в своем роде технологию снятия "отпечатков пальцев" и сравнения видео на **YouTube**, которая сканирует и идентифицирует загруженные видео, содержащие известные материалы, связанные с сексуальными злоупотреблениями в отношении детей.

Во время хакатона по безопасности детей в 2019 году **Facebook** объявил о переводе на открытый исходный код двух технологий, которые обнаруживают идентичные и почти идентичные фотографии и видео. Эти два алгоритма доступны на GitHub, что позволяет системам обмена хэшами общаться друг с другом и делает системы намного более мощными.

Горячая линия организации IWF постоянно функционирует и не только следит за тысячами сообщений от представителей общественности, которые натолкнулись на онлайновые изображения, содержащие элементы сексуальных злоупотреблений в отношении детей, но и выполняет уникальную инициативную роль, осуществляя поиск этого незаконного контента в интернете. Возможность использовать информацию горячих линий и фокусировать ресурсы на ней позволяет идентифицировать и удалить больше контента. Более того, IWF неизменно работает с Google, Microsoft, Facebook и другими компаниями, являющихся ее членами, чтобы постоянно расширять технические границы. IWF предлагает в качестве решения портал для направления сообщений, который дает возможность пользователям интернета в странах без горячих линий сообщать об изображениях и видеороликах, содержащих предполагаемые элементы сексуальных злоупотреблений в отношении детей, непосредственно в IWF через специальную страницу онлайнового портала.

IWF в сотрудничестве с благотворительным Фондом Мэри Коллинз, специализирующемся на поддержке жертв, хочет запустить новую кампанию, в которой будет призывать молодых мужчин сообщать о любых самостоятельно генерированных сексуальных изображениях или видеороликах детей до 18 лет, с которыми они сталкиваются при навигации по интернету.

В **Интерполе** создана Международная база данных по сексуальной эксплуатации детей (ICSE), содержащая изображения и видео, – инструмент разведки и расследования, который позволяет специализированным следователям более чем из 50 стран обмениваться данными о случаях сексуальных злоупотреблений в отношении детей. Анализируя цифровой, визуальный и звуковой контент фотографий и видео, определяющие жертв специалисты могут находить улики, выявлять любые совпадения в делах и объединять усилия по поиску жертв сексуальных злоупотреблений в отношении детей. В настоящее время база данных Интерпола по сексуальной эксплуатации детей содержит более 1,5 млн. изображений и видео, и благодаря ей было найдено 19 400 жертв по всему миру.

NetClean ProActive – это программное обеспечение, основанное на сопоставлении сигнатур и других алгоритмах обнаружения, которые автоматически обнаруживают изображения и видео, содержащие элементы сексуальных злоупотреблений в отношении детей, в корпоративной среде.

Компания **Griffeye Brain** использует искусственный интеллект для сканирования контента, не относившегося ранее к какой-либо категории, сравнения его с атрибутами известного контента CSAM и пометки подозрительных элементов для просмотра агентом.

Организация RAINN создала Национальную горячую линию по борьбе с сексуальным насилием, управляет ее работой в партнерстве более чем с 1000 местных организаций по всей стране, которым можно сообщить о случае сексуального насилия, а также администрирует службу Безопасного телефона доверия Министерства обороны США. RAINN также осуществляет программы по предотвращению сексуального насилия, оказанию помощи пострадавшим и обеспечению привлечения виновных к ответственности.

Safehorizon – это некоммерческая организация по оказанию помощи жертвам насилия и злоупотреблений, которая работает в Нью-Йорке с 1978 года. Safehorizon оказывает жертвам насилия услуги горячей линии.

Project Arachnid – это инновационный инструмент, который администрируют в Канаде, служащий для борьбы с растущим распространением в интернете материалов, связанных с сексуальными злоупотреблениями в отношении детей (CSAM).

[i] http://www.oecd.org/internet/bridging-the-digital-gender-divide.pdf.

При поддержке:

With the support of:

Международный
союз
электросвязи
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN: 978-92-61-30454-6

Опубликовано в Швейцарии
Женева, 2020 г.

Фотографии представлены: Shutterstock