ITUПубликации

Международный союз электросвязи
Сектор развития

Руководящие указания для отрасли по защите ребенка в онлайновой среде

2020

ITU

Руководящие указания для отрасли по защите ребенка в онлайновой среде

Выражение признательности

Настоящие Руководящие указания разработаны Международным союзом электросвязи (МСЭ) и рабочей группой авторов, направляющих вклады от ведущих организаций, представляющих сектор информационно-коммуникационных технологий (ИКТ) и занимающихся вопросами защиты детей, включая EPC, Глобальное партнерство по прекращению насилия в отношении детей, Ассоциация GSM, Международный союз инвалидов, Internet Watch Foundation (IWF), Privately SA и ЮНИСЕФ. Рабочую группу возглавлял Аньян Босе (ЮНИСЕФ), а ее работу координировала Фанни Ротино (МСЭ).

Публикация настоящих Руководящих указаний МСЭ была бы невозможной без энтузиазма, преданности и времени, затраченного направившими свои вклады авторами. Неоценимые вклады также были получены от e-Worldwide Group (e-WWG), Facebook, Tencent Games, Twitter, The Walt Disney Company и других заинтересованных сторон в отрасли, которые разделяют общую задачу, предполагающую сделать интернет более безопасным местом для детей и молодых людей. Ниже перечислены партнеры, которым МСЭ выражает благодарность за то, что они уделили свое драгоценное время и поделились своими взглядами (перечисление приводится в алфавитном порядке по названию организаций):

- Джакомо Мадзоне (EPC)
- Сальма Аббаси (e-WWG)
- Дэвид Майлз и Каролин Херст (Facebook)
- Эми Крокер и Серена Томмасино (Глобальное партнерство по прекращению насилия в отношении детей)
- Дженни Джоунс (SMA)
- Люси Ричардсон (Международный союз инвалидов)
- Фанни Ротино (МСЭ)
- Тесс Лейланд (IWF)
- Дипак Тевари (Privately SA)
- Адам Луи (Tencent Games)
- Кати Миншелл (Twitter)
- Аньян Босе, Дэниель Кардефельт Винтер, Эмма Дэй, Джозианна Галеа Барон, Сара Якобштейн и Стивен Эдвин Вослоо (ЮНИСЕФ)
- Эми Э. Каннингхэм (The Walt Disney Company)

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

Стремительное развитие цифровых технологий привело к появлению беспрецедентных возможностей для детей и молодежи в плане общения, установления связей, обучения, обмена информацией и доступа к ней, а также выражения своих взглядов и мнений по вопросам, затрагивающим их жизни и их сообщества.

Но вместе с тем более широкий и легкий доступ к онлайновым услугам представляет более серьезную угрозу для безопасности детей как в онлайновой среде, так и в реальной жизни. Современные дети сталкиваются со множеством серьезных рисков – от вопросов неприкосновенности частной жизни, насилия между сверстниками и жестокого и/или не соответствующего возрасту контента до интернет-мошенничества и преступлений против детей, таких как груминг в онлайновой среде и сексуальные злоупотребления и сексуальная эксплуатация. Угрозы множатся, а правонарушители все чаще действуют одновременно, находясь при этом в разных странах, что усложняет их отслеживание и привлечение к ответственности.

Помимо этого, глобальная пандемия COVID-19 привела к увеличению числа детей, впервые начавших пользоваться интернетом для продолжения своего образования и поддержания социального взаимодействия. Ограничения, обусловленные вирусом, означают не только то, что много детей более юного возраста начинают общаться в сети гораздо раньше, чем, возможно, планировали их родители, но и то, что ввиду необходимости пересмотра своих рабочих обязательств многие родители оказались не в состоянии контролировать своих детей, подвергая их риску доступа к неприемлемому контенту или превращения в мишень для преступников, производящих материалы, связанные с сексуальными злоупотреблениями в отношении детей (CSAM).

Преступники получают выгоду от технологического прогресса, например приложений и игр, обеспечивающих взаимодействие, быстрого обмена файлами, потокового вещания, криптовалют, теневого интернета и программ устойчивого шифрования. При этом они также извлекают выгоду из зачастую нескоординированных и нерешительных действий по эффективному устранению проблемы со стороны технологического сектора.

Отчасти проблему можно решить благодаря появляющимся технологиям, например с использованием обслуживаемой искусственным интеллектом базы данных Интерпола по сексуальным злоупотреблениям в отношении детей, в которой применяется программное обеспечение для сравнения изображений и видеоматериалов, позволяющее быстро установить связи между жертвами, насильниками и их местоположением. Однако одних только технологий недостаточно для решения проблемы.

Для снижения рисков, связанных с цифровой революцией, при одновременном обеспечении возможностей для использования ее преимуществ все большим числом молодых людей как никогда прежде важна совместная и скоординированная реакция различных заинтересованных сторон. Правительства, гражданское общество, местные сообщества, международные организации и заинтересованные стороны отрасли должны объединить свои усилия ради общей цели.

Признавая этот факт, в 2018 году Государства – Члены МСЭ обратились с просьбой подготовить развернутое обновление наших Руководящих указаний по защите ребенка в онлайновой среде. Эти новые Руководящие указания МСЭ были переосмыслены, переформулированы и перестроены с учетом произошедших значительных изменений в цифровой среде, в которой живет нынешнее поколение детей. Помимо включения новых разработок в сфере цифровых технологий и платформ, в данном новом издании устраняется значительный пробел: в нем уделяется внимание положению детей-инвалидов, для которых онлайновая среда открывает особенно важные возможности по обеспечению полноценного участия в социальной жизни.

Отрасль электронных технологий играет решающую и инициативную роль в формировании основ более безопасного и надежного использования интернет-услуг и других технологий для современных детей и будущих поколений.

Любая предпринимательская деятельность должна активнее ориентироваться на интересы детей с особым акцентом на защиту персональных данных юных пользователей, сохранение их права на свободу выражения своего мнения, борьбу с растущими объемами CSAM и обеспечение систем эффективного противодействия нарушению прав детей и реагирования на факты совершения таких нарушений.

В тех странах, где нормы местного законодательства пока отстают от требований международного права, все предприятия имеют возможности и одновременно обязанности по согласованию своих собственных методов работы с высокими стандартами и передовым опытом.

Мы надеемся, что для отрасли эти Руководящие указания послужат прочной основой для разработки правил ведения бизнеса и инновационных решений. Я горжусь тем, что эти Руководящие указания являются результатом совместной работы на общемировом уровне и их соавторами являются специалисты из широкого международного сообщества, что соответствует истинному назначению МСЭ как глобального организатора.

Я также рада представить новый талисман COP – Санго – дружелюбного, непоседливого и отважного персонажа, созданного группой детей в рамках новой международной программы МСЭ по охвату молодежи.

В эпоху, когда все больше молодых людей подключаются к интернету, Руководящие указания МСЭ по защите ребенка приобретают особую значимость. Отрасль, правительства, родители и педагоги, а также сами дети – все должны сыграть свою важную роль. Я, как всегда, очень благодарна вам за поддержку и с нетерпением жду продолжения нашего тесного сотрудничества в решении данных насущных вопросов.

Дорин Богдан-Мартин
Директор
Бюро развития электросвязи, МСЭ

Содержание

Таблицы

1 Обзор

Цель настоящего документа – задать направление для заинтересованных сторон отрасли ИКТ в плане создания их собственных ресурсов по защите детей в онлайновой среде (СОР). Данные Руководящие указания по защите ребенка в онлайновой среде предназначены для отрасли и призваны составить полезную, гибкую и удобную в применении основу как для разработки концепций различных компаний, так и для формирования их ответственности в области защиты пользователей. Они также направлены на формирование основ более безопасного и надежного использования интернет-услуг и других технологий для современных детей и будущих поколений.

Являясь набором инструментов, настоящие Руководящие указания также имеют целью способствовать успешности бизнеса, помогая крупным и мелким оператором и заинтересованным сторонам в разработке и поддержании привлекательных и устойчивых бизнес-моделей, одновременно осознавая правовую и моральную ответственность перед детьми и обществом.

Реагируя на значительный прогресс в сфере технологий и их конвергенцию, МСЭ, ЮНИСЕФ и партнеры по защите ребенка в онлайновой среде разработали и обновили Руководящие указания для широкого спектра компаний, занимающихся разработкой, предоставлением или использованием технологий электросвязи при распространении своей продукции и услуг.

Новые Руководящие указания для отрасли по защите ребенка в онлайновой среде являются результатом консультаций с участниками Инициативы СОР, а также более широкого консультационного процесса с участием гражданского общества, бизнеса, сферы образования, государственных органов, средств массовой информации, международных организаций и молодых людей.

Цели настоящего документа:

- определить общий эталон и руководящие указания для отраслей, связанных с ИКТ и интернетом, а также для всех заинтересованных сторон;
- предоставить компаниям руководящие указания по выявлению, предотвращению и смягчению любого рода негативного влияния их продукции и услуг на права детей;
- предоставить компаниям руководящие указания по выявлению способов содействия реализации прав ребенка и формированию ответственного цифрового гражданства среди детей;
- предложить общие принципы для формирования основы национальных или региональных обязательств по всем взаимосвязанным отраслям, одновременно осознавая, что разные типы бизнеса используют разные модели их исполнения.

Сфера применения

Защита ребенка в онлайновой среде – это комплексная задача, охватывающая множество разных управленческих, политических, оперативных, технических и правовых аспектов. Настоящие Руководящие указания являются попыткой проанализировать, организовать и определить приоритеты многих из таких аспектов на основании признанных моделей, схем и прочих материалов.

Руководящие указания направлены на защиту детей во всех областях и от всех рисков цифрового мира и, как таковые, выделяют передовой опыт отраслевых заинтересованных сторон, который можно учитывать в процессе проектирования, разработки и управления политиками СОР на уровне компаний. Они задают направление для участников отрасли не только в том, как управлять и сдерживать незаконную онлайновую деятельность, которой они обязаны противодействовать (например, CSAM в интернете) посредством своих услуг, но и в том, как подходить к решению других вопросов, которые могут не считаться преступлениями в разных юрисдикциях. К ним относятся насилие между сверстниками, кибертравля и домогательства в интернете, а также вопросы, связанные с конфиденциальностью или общим благополучием, мошенничеством или другими угрозами, которые могут лишь навредить детям в определенном контексте.

В этой связи в Руководящие указания включены рекомендации относительно передовых практических подходов к устранению рисков, с которыми сталкиваются дети в цифровом мире, и того, как действовать в целях формированию безопасной среды для детей в интернете. В них содержатся советы по методам работы отрасли, способствующим обеспечению безопасности детей, пользующихся ИКТ, интернетом и всеми сопутствующими технологиями или устройствами, имеющими выход в интернет, включая мобильные телефоны, игровые консоли, игрушки, имеющие выход в интернет, часы, интернет вещей и

системы, управляемые ИИ. Таким образом, они содержат обзор ключевых аспектов и задач, связанных с защитой ребенка в онлайновой среде и предложения по действиям, которые бизнес и заинтересованные лица могут предпринять для разработки местных и внутренних политик СОР. Эти Руководящие указания не охватывают таких моментов, как фактическая разработка процесса или конкретный текст политик СОР для отрасли.

Структура

Раздел 1 – Обзор. В этом разделе определены цель, сфера применения и целевая аудитория данных Руководящих указаний.

Раздел 2 – Введение в тему защиты ребенка в онлайновой среде. В этом разделе представлен обзор темы защиты ребенка в онлайновой среде и некоторая базовая информация, включая особую ситуацию, в которой находятся дети-инвалиды. Кроме того, здесь приводятся примеры существующих международных и национальных моделей по обеспечению безопасности детей в онлайновой среде как вероятной сферы вмешательства для заинтересованных сторон в отрасли.

Раздел 3 – Основные области в сфере защиты и содействия реализации прав детей. Этот раздел посвящен описанию пяти основных вариантов действий компаний в направлении обеспечения защиты детей и позитивного применения ИКТ.

Раздел 4 – Общие руководящие указания. В этом разделе даны рекомендации для всех заинтересованных сторон в отрасли по обеспечению безопасности детей при использовании ИКТ и по содействию позитивному применению ИКТ, включая ответственное цифровое гражданство среди детей.

Раздел 5 – Контрольные перечни в зависимости от выполняемых функций. Этот раздел содержит отдельные рекомендации для заинтересованных сторон по конкретным действиям в отношении поддержки прав детей с учетом следующих функций:

- функция A: предоставление услуг установления соединений, хранения и размещения данных;
- функция B: предложение отобранного цифрового контента;
- функция C: размещение создаваемого пользователями контента и установление связей между пользователями;
- функция D: системы на основе искусственного интеллекта.

Целевая аудитория

В контексте разработанных ООН Руководящих принципов предпринимательской деятельности в аспекте прав человека[1] документ "Права детей и принципы предпринимательства" призывает компании выполнять свои обязательства по уважению прав детей, избегая любого рода негативных воздействий в связи с их деятельностью, продукцией или услугами. Принципы устанавливают различие между "уважением" (минимальным требованием к компаниям по недопущению нанесения вреда детям) и "поддержкой" (выражающейся, например, в проведении добровольных акций, направленных на обеспечение реализации прав ребенка). Компании должны обеспечивать права детей как на защиту в онлайновой среде, так и на доступ к информации и свободу выражения, содействуя, при этом, позитивному применению ИКТ детьми.

Традиционное разграничение между различными сферами отраслей электросвязи и подвижной связи, а также между интернет-компаниями и радиовещательными организациями стремительно рушится или становится несущественным. Конвергенция ведет к объединению этих ранее четко разделенных цифровых потоков в одно течение, охватывающее миллиарды людей во всех уголках мира. Кооперация и партнерство являются ключами к формированию основ более безопасного и надежного использования интернета и сопутствующих технологий. Государственные органы, частный сектор, директивные органы, сфера образования, гражданское общество, родители и опекуны – все они играют предельно важную роль в достижении поставленной цели. Отрасль может действовать в пяти основных областях, описание которых приводится далее в разделе 3.

[1] Организация Объединенных Наций "Руководящие принципы предпринимательской деятельности в аспекте прав человека".

2 Что такое защита ребенка в онлайновой среде?

За последние 10 лет характер использования и роль интернета в жизни людей значительно изменились. Учитывая преобладание смартфонов и планшетов, доступность Wi-Fi и технологий 4G, а также развитие платформ социальных сетей и приложений, все больше людей получают доступ к интернету в силу различных причин, количество которых постоянно растет.

В 2019 году более половины всего населения Земли пользовались интернетом. Крупнейшую часть пользователей интернета составляют люди в возрасте моложе 44 лет, при этом объемы использования в возрастных группах 16–24 года и 35–44 года одинаковы. На глобальном уровне каждый третий пользователь интернета является ребенком (0–18 лет), и по оценкам ЮНИСЕФ 71 процент молодых людей уже находятся в онлайновой среде[2]. Повсеместное распространение точек доступа к интернету, подвижные технологии и растущее многообразие устройств на базе интернет-технологий (в сочетании с громадными ресурсами киберпространства) создают беспрецедентные возможности для обучения, обмена информацией и общения.

К преимуществам использования ИКТ относятся более широкий доступ к информации о социальных службах, образовательных ресурсах и здоровье. Поскольку дети, молодые люди и семьи пользуются интернетом и мобильными телефонами для поиска информации и помощи, а также для сообщения о случаях злоупотреблений, такие технологии способны помочь защитить детей и молодых людей от насилия и эксплуатации. Поставщики услуг защиты детей также используют ИКТ, среди прочего, для сбора и передачи данных, тем самым упрощая регистрацию рождения, управление делами, отслеживание семей, сбор данных и составление карт насилия.

Помимо того, интернет обеспечил более свободный доступ к информации во всех уголках земного шара, предоставляя детям и молодым людям возможность изучить практически любой интересующий их предмет, получить доступ ко всемирным средствам массовой информации, отследить предлагаемые вакансии и освоить идеи для будущего. Применение ИКТ дает детям и молодым людям возможность заявить о своих правах и выразить свое мнение, а также предлагает множество способов установления контактов и общения с их семьями и друзьями. ИКТ также выступают в качестве первостепенного средства культурного обмена и источника развлечений.

Несмотря на серьезные преимущества интернета, пользуясь ИКТ, дети и молодые люди также сталкиваются со множеством рисков. Они могут подвергаться воздействию не соответствующего их возрасту контента или неприемлемых контактов, включая возможных виновников сексуальных злоупотреблений. Они могут страдать от подрыва репутации в результате публикации персональной информации интимного характера либо в интернете, либо посредством "секстинга", не сумев в полной мере понять все последствия подобных контактов для самих себя и других лиц в их долгосрочной "цифровой географии". Они также сталкиваются с риском нарушения конфиденциальности, связанным со сбором и использованием данных, а также сбором информации о местонахождении.

Конвенция о правах ребенка, являющаяся наиболее широко ратифицированным международным документом по правам человека[3], дает определение гражданских, политических, экономических, социальных и культурных прав детей. В ней зафиксировано, что все дети имеют право на образование; досуг, участие в играх и культурной жизни; получение соответствующей информации; свободу мысли и выражения; личную жизнь и выражение своих взглядов по затрагивающим их вопросам в соответствии с их развивающимися способностями. Кроме того, Конвенция защищает детей от всех форм насилия, эксплуатации, злоупотребления и дискриминации любого рода и гарантирует решение всех касающихся их вопросов с учетом наилучших интересов ребенка. Родители, опекуны, педагоги и представители сообществ, включая лидеров сообществ и различных общественных деятелей несут ответственность по воспитанию и поддержке детей и молодых людей по мере их взросления. Государственные органы играют важную роль в обеспечении того, чтобы все заинтересованные стороны выполняли свои задачи.

[2] OECD, "New Technologies and 21st Century Children: Recent Trends and Outcomes", Education Working Paper No. 179.

[3] Организация Объединенных Наций, Конвенция о правах ребенка. Все страны, кроме трех (Сомали, Южный Судан и США), ратифицировали Конвенцию о правах ребенка.

В отношении защиты прав детей в онлайновой среде бизнесу необходимо объединять усилия в поисках точного баланса между правом ребенка на защиту и правами на доступ к информации и свободное выражение своего мнения. Компаниям следует поставить на одно из первых мест меры по защите детей в онлайновой среде, которые должны быть целенаправленными и без чрезмерных ограничений как для ребенка, так и для других пользователей. Кроме того, все более укрепляется общее мнение о том, что содействие цифровому гражданству среди детей и молодежи, а также разработка продуктов и платформ, содействующих позитивному применению ИКТ детьми должны стать приоритетом для частного сектора.

Притом что интернет-технологии создают множество возможностей для детей и молодых людей в плане общения, изучения новых навыков, творчества и вклада в улучшение общества для всех, они также могут представлять новые риски для безопасности детей и молодых людей. Они могут подвергать детей и молодых людей потенциальным рискам и наносить вред в таких сферах так конфиденциальность, незаконный контент, домогательство, кибертравля, неправомерное использование персональных данных или груминг в сексуальных целях и даже сексуальные злоупотребления в отношении детей и их сексуальная эксплуатация. Помимо этого, они могут наносить ущерб репутации, включая "порноместь" в связи с публикацией закрытой персональной информации либо в интернете, либо с применением "секстинга" как способа, посредством которого пользователи могут рассылать сексуально откровенные сообщения, фотографии или изображения между мобильными телефонами. Также существуют риски, связанные с конфиденциальностью при использовании интернета. Дети в силу их возраста и недостаточной зрелости часто неспособны полностью понять риски, с которыми сопряжен онлайновый мир, и вероятные негативные последствия их неприемлемого поведения для других и их самих.

Несмотря на все преимущества, есть также и обратная сторона использования появляющихся и более продвинутых технологий. Разработки в области ИИ и машинного обучения, виртуальной и дополненной реальности, больших данных, робототехники и интернета вещей еще больше преобразуют взаимодействие детей и молодых людей со средствами передачи. Притом что такие технологии разрабатываются, главным образом, с целью расширения объема предоставляемых услуг и повышения удобства (с помощью, например, голосовых ассистентов, доступности и новых форм цифрового погружения), некоторые из них могут иметь непреднамеренное влияние и даже неправомерно использоваться лицами, совершающими сексуальные преступления против детей, в целях удовлетворения их потребностей. Создание безопасной и надежной онлайновой среды для детей и молодых людей требует эффективного участия государственных органов, частного сектора и всех заинтересованных лиц. Кроме того, одной из первостепенных целей должно быть развитие цифровых навыков и грамотности у родителей и преподавателей, и в ее достижении отрасль может играть жизненно важную и устойчивую роль.

Некоторые дети могут хорошо понимать онлайновые риски и знать, как реагировать на них. Тем не менее, этого нельзя сказать обо всех детях повсеместно, особенно среди уязвимых групп. Согласно задаче 16.2, поставленной в рамках Целей ООН в области устойчивого развития, которая направлена на устранение злоупотреблений, эксплуатации, торговли людьми и всех форм насилия и пыток в отношении детей, защита детей в онлайновой среде имеет огромное значение.

Начиная с 2009 года организованная МСЭ Инициатива СОР для множества заинтересованных сторон на международном уровне служила цели повышения осведомленности о безопасности детей в онлайновой среде и реагирования на эти риски. Она направлена на объединение усилий партнеров из всех секторов мирового сообщества с целью обеспечения безопасного и надежного онлайнового опыта для детей в любой точке мира. В части этой Инициативы в 2009 году МСЭ опубликовал набор Руководящих указаний СОР для четырех групп: детей; родителей, опекунов и педагогов; отрасли; директивных органов. В данных

Руководящих указаниях защита ребенка в онлайновой среде понимается как всеохватный подход к реагированию на все потенциальные угрозы и вред, с которыми дети и молодые люди могут столкнуться либо в онлайновой среде, либо при содействии онлайновых технологий. В этом документе защита ребенка в онлайновой среде также включает вред, наносимый детям в реальном мире, но связанный со свидетельствами онлайнового насилия и злоупотреблений. Кроме рассмотрения поведения и действий детей в интернете, защита ребенка в онлайновой среде также включает неправомерное использование технологий другими лицами, помимо самих детей, с целью эксплуатации детей.

Все соответствующие заинтересованные стороны выполняют определенные роли в том, чтобы помочь детям и молодым людям воспользоваться возможностями, предлагаемыми интернетом, приобретая, при этом, цифровую грамотность и стойкость в отношении онлайнового благополучия и защиты.

Защита детей и молодых людей является общей обязанностью всех заинтересованных сторон. Для практического решения этой задачи директивные органы, представители отрасли, родители, опекуны, педагоги и другие заинтересованные стороны должны обеспечить детям и молодым людям возможность реализации своего потенциала как в онлайновой среде, так и в реальной жизни.

При отсутствии универсального определения защита ребенка в онлайновой среде принимает форму целостного подхода к созданию безопасного, соответствующего возрасту, инклюзивного и предполагающего участие цифрового пространства для детей и молодых людей, которое имеет следующие характеристики:

- реагирование, поддержка и самопомощь перед лицом угроз;
- предотвращение вреда;
- динамичный баланс между обеспечением защиты и предоставлением детям возможности стать цифровыми гражданами;
- соблюдение прав и обязанностей как со стороны детей, так и со стороны общества.

Более того, ввиду стремительного развития технологий и общества, а также отсутствия границ в интернете защита детей в онлайновой среде, чтобы быть эффективной, должна быть быстрой и адаптивной. По мере развития технологических инноваций будут появляться новые задачи, характер которых будет зависеть от региона. Объединение усилий в рамках глобального сообщества является лучшим способом их успешного решения, учитывая необходимость поиска новых подходов.

2.1 Базовая информация

Поскольку интернет полностью интегрирован в жизнь детей и молодых людей, нельзя рассматривать цифровой и физический мир раздельно.

Такая возможность установления соединений открывает невероятные перспективы. Мир интернета позволяет детям и молодым людям преодолевать неблагоприятные обстоятельства и ограниченность возможностей, а также служит новой ареной для развлечений, обучения, участия и формирования взаимоотношений. Нынешние цифровые платформы используются для самых разных видов деятельности, и получаемый опыт часто является мультимедийным.

Доступ и обучение использованию таких технологий и ориентации в них рассматриваются как критически важные навыки для развития молодых людей, и первое использование ИКТ происходит в раннем возрасте. Таким образом, очень важно, чтобы все действующие лица осознавали, что дети и молодые люди часто начинают пользоваться платформами и услугами до того, как достигнут определенного минимального возраста, которому технологическая отрасль обязана соответствовать, и поэтому обучение, наряду с мерами защиты, должно быть интегрировано во все онлайновые услуги, используемые детьми.

2.1.1 Дети в цифровом мире

Доступ к интернету

По данным за 2019 год более половины населения Земли пользовались интернетом (53,6 процента), что по расчетам составляет 4,1 миллиарда пользователей. На глобальном уровне каждый третий пользователь интернета является ребенком в возрасте моложе 18 лет[1]. Согласно данным ЮНИСЕФ по всему миру 71 процент молодых людей уже подключены к интернету[2]. Несмотря на установленный минимальный возраст, Ofcom (регуляторный орган отрасли связи Соединенного Королевства,) полагает, что порядка 50 процентов детей в возрасте от 10 до 12 лет уже имеют свою учетную запись в социальных сетях[3]. Дети и молодые люди сегодня имеют значительное, постоянное и стабильное присутствие в интернете. Интернет-услуги, ориентированные на иные цели, кроме социальных, экономических и политических, стали семейным или потребительским продуктом или услугой, являющейся неотъемлемой частью жизни семей, детей и молодых людей.

В 2017 году на региональном уровне доступ детей и молодых людей в интернет был прочно связан с уровнем национального дохода. В странах с низким доходом наблюдался более низкий показатель количества детей, пользующихся интернетом, по сравнению со странами с высоким доходом. Дети и молодые люди в большинстве стран проводят больше времени в сети по выходным, чем в будние дни, при этом подростки в возрасте от 15 до 17 лет тратят на интернет больше времени, чем другие группы, находясь в сети порядка 2,5 – 5,3 часа в зависимости от страны.

---

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 BBC, "Under-age social media use 'on the rise', says Ofcom".

Использование интернета

Самым популярным устройством для доступа к интернету среди детей и молодежи является мобильный телефон. На втором месте находятся персональные компьютеры и ноутбуки. Дети и молодые люди проводят в сети, в среднем, два часа в день в течение недели и четыре часа каждый день на выходных. Притом что часть из них считает себе постоянно соединенными, многие все еще не имеют доступа к интернету дома. На практике большинство детей и молодых людей, которые пользуются интернетом, получают доступ через более чем одно устройство – те, кто соединяется, по крайней мере, еженедельно, иногда пользуются тремя разными устройствами. Дети более старшего возраста и те, кто живет в более богатых странах, обычно пользуются бóльшим количеством устройств, при этом мальчики используют несколько больше устройств, чем девочки во всех обследованных странах.

Наиболее популярным видом деятельности как среди мальчиков, так и среди девочек является просмотр видеороликов. Более трех четвертей детей и молодых людей, пользующихся интернетом, сообщили о том, что просматривают видео в сети как минимум каждую неделю либо самостоятельно, либо с другими членами семьи. Многих детей и молодых людей можно назвать "активно общающимися", поскольку они пользуются несколькими социальными сетями, такими как Facebook, Twitter, Tiktok или Instagram. Дети и молодые люди также участвуют в политической жизни в интернете и делятся своим мнением с помощью блогов.

Общий уровень участия в онлайновых играх зависит от страны и грубо соотносится с показателем легкости доступа к интернету для детей и молодых людей. Тем не менее, доступность онлайновых игр и их приемлемость в ценовом отношении быстро меняются, и возраст детей, впервые получающих доступ к онлайновым играм, снижается.

Еженедельно 10 – 30 процентов пользующихся интернетом детей и молодых людей из числа опрошенных в ряде стран участвуют в творческой деятельности в онлайновой среде[1]. В образовательных целях многие дети и молодые люди всех возрастов каждую неделю пользуются интернетом для выполнения домашних заданий или даже для наверстывания пропущенных уроков или в поисках информации о здоровье. Более старшие дети, похоже, проявляют больше интереса к информации, чем дети помоложе.

[1] 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.

Сексуальная эксплуатация и сексуальные злоупотребления в отношении детей в онлайновой среде

Сексуальная эксплуатация и сексуальные злоупотребления в отношении детей (CSEA) в онлайновой среде растут ошеломляющими темпами. Десять лет назад сообщалось о менее чем одном миллионе файлов, содержащих материалы, связанные со злоупотреблениями в отношении детей. В 2019 году их число выросло до 70 миллионов, причем этот показатель вырос почти на 50 процентов за один только 2018 год. Кроме того, впервые количество видеоматериалов превысило количество фотог

рафий согласно данным, полученным властями, что говорит о необходимости поиска новых инструментов для сдерживания данной тенденции. Жертвы CSEA в интернете относятся к разным возрастным группам, но все больше молодеют. В 2018 году аналитики сети горячих линий INHOPE отметили смещение в профилях жертв с подросткового к предподростковому возрасту. Кроме того, по данным исследования, проведенного ECPAT International и Интерполом в 2018 году, дети более юного возраста, вероятнее всего, подвергаются более серьезным злоупотреблениям, включая пытки, жесткое изнасилование или садизм. В том числе это относится к младенцам в возрасте всего лишь нескольких дней, недель или месяцев. Притом что чаще всего жертвами становятся девочки, мальчики могут подвергаться более жестокому насилию. В том же отчете отмечено, что 80 процентов жертв, о которых сообщалось, были девочками, а 17 процентов – мальчиками. Дети обоих полов упоминались в 3 процентах сообщений[1].

[1] ECPAT and Interpol, “Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material: summary report”, 2018.

Срез данных[1]

- Каждый третий пользователь интернета во всем мире является ребенком.
- Каждые полсекунды один ребенок подключается к интернету в первый раз.
- 800 миллионов детей пользуются социальными сетями.
- По имеющимся оценкам в любой момент времени 750 000 человек, находящихся в сети, ищут соединения с детьми в сексуальных целях.
- В хранилище Европола содержится более 46 миллионов уникальных изображений или видеороликов со CSAM.
- Возраст более 89 процентов жертв составляет от 3 до 13 лет.

Более подробная информация о масштабах и методах реагирования на CSEA в интернете приводится на сайте Глобального альянса WePROTECT.

[1] Сайт Фонда по прекращению насилия в отношении детей (End Violence Against Children), “Safe Online”.

2.1.2 Влияние разных платформ на цифровой опыт детей

Интернет и цифровые технологии представляют как возможности, так и риски для детей и молодых людей. Некоторые из них перечислены ниже.

Когда дети пользуются **социальными сетями**, они получают преимущества, связанные со множеством возможностей исследовать, учиться, общаться и развивать ключевые навыки. Для детей социальные сети служат платформой, позволяющей им исследовать собственную личность в безопасной среде. Для молодых людей крайне важно обладать соответствующими навыками и знать, как решать вопросы, связанные с конфиденциальностью и репутацией.

"Я знаю – все, что ты постишь в интернете остается там навсегда и может в будущем повлиять на твою жизнь", – 14-летний мальчик из Чили.

Тем не менее, учитывая, что по данным многих обследований большинство детей начинают пользоваться социальными сетями, не достигнув минимального возраста 13 лет, а средства проверки возраста, в целом, либо слабые, либо отсутствуют, дети сталкиваются с очень серьезными рисками. Кроме того, притом что дети хотят осваивать цифровые навыки, становиться цифровыми гражданами и контролировать настройки конфиденциальности, они склонны рассматривать конфиденциальность исключительно в отношении своих друзей и знакомых – "что могут увидеть мои друзья", – но без учета незнакомых людей и третьих сторон. Это, в сочетании с природным любопытством детей и закономерно более низкими порогами восприятия риска, способно сделать их уязвимыми для груминга, эксплуатации, травли и других типов вредного контента и контактов.

Широкая популярность обмена изображениями и видеоматериалами через мобильные приложения и, в особенности, использование платформ прямого потокового вещания, создают дополнительные поводы для беспокойства о конфиденциальности и риски. Некоторые дети делают сексуальные фотографии самих себя, своих друзей и братьев или сестер и делятся ими в интернете. В 2019 году почти треть (29 процентов) все веб-страниц, подписанных IWF, содержала самостоятельно выполненные изображения. На 76 процентах таких изображений были представлены девочки в возрасте 11–13 лет, причем большинство из них фотографировались в своей ванной комнате или другой комнате своего дома. Для одних, особенно более старших детей, это может быть проявлением естественного исследования сексуальности и сексуальной идентичности, тогда как для других, особенно детей более юного возраста, это зачастую связано с принуждением со стороны взрослых или других детей. Как бы там ни было, итоговый контент во многих странах является незаконным и может подвергать ребенка риску уголовного преследования или использования для дальнейшей эксплуатации, груминга или принуждения.

Аналогично, **онлайновые игры** позволяют детям реализовать свое фундаментальное право на игру, а также создавать коммуникационные сети, проводить время с друзьями и общаться с ними, развивая важные навыки. При всей преобладающей позитивности в некоторых случаях игровые платформы, если их использование детьми не контролируется ответственными взрослыми, которые не оказывают детям необходимой поддержки, могут также представлять риск. К нему относятся чрезмерное количество времени, проводимое за играми, финансовые риски, связанные с крупными покупками внутри игры, сбор и монетизация персональных данных ребенка участниками отрасли, кибертравля, язык ненависти, насилие и подверженность неприемлемому поведению или контенту, груминг, использование реальных, созданных компьютером или даже виртуальной реальностью изображений, а также видеоролики, изображающие и утверждающие CSEA в качестве нормы. Эти риски не уникальны для игровой среды, и также применяются к другим цифровым средам, в которых дети могут проводить время.

Кроме того, технологические разработки привели к появлению "**интернета вещей**", позволяющего самым разным устройствам, подключенным к интернету, количество которых постоянно растет, соединяться между собой и формировать сети в интернете. К ним, в частности, относятся игрушки, радио-няни и устройства, управляемые ИИ, которые могут представлять риск в отношении конфиденциальности и нежелательных контактов.

Передовой опыт: исследования

Применительно к вопросу травли в онлайновой среде или кибертравли компания Microsoft провела исследование по цифровой безопасности и кибертравле. В 2012 году исследователи опросили детей из 25 стран в возрасте от 8 до 17 лет об их негативном опыте в интернете. Полученные результаты показали, что в среднем 54 процента участников отметили, что их беспокоила вероятность травли в онлайновой среде, 37 процентов заявили, что подвергались кибертравле и 24 процента признались, что сами дразнили кого-то другого. В рамках того же исследования выяснилось, что менее трех из 10 родителей обсуждали травлю в онлайновой среде со своими детьми. Начиная с 2016 года Microsoft проводит **регулярные исследования** по теме онлайновых рисков, ежегодно составляя отчеты по Индексу цифровой культуры.

FACES является мультимедийной программой, выпускаемой каналом NHK, Япония, и консорциумом различных компаний общественного вещания, в рамках которой рассказываются истории жертв травли в онлайновой среде и в реальной жизни по всему миру. Это серия личных историй подростков, в которых главные герои перед камерой делятся тем, как они реагировали на нападки в интернете. Такую же серию, выпускаемую в форме двухминутных клипов, запустили Facebook, ЮНЕСКО и Совет Европы. Эти ролики можно посмотреть на нескольких языках.

В 2019 году ЮНИСЕФ опубликовал дискуссионный документ под заголовком Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry ("Права ребенка и онлайновые игры: возможности и сложности для детей и отрасли"), чтобы обсудить возможности и сложности, возникающие перед детьми в одной из наиболее быстро растущих отраслей развлечений. В документе рассматриваются следующие темы:

- право детей на игру и свободу выражения (время, проводимое за игрой, и последствия для здоровья);
- отсутствие дискриминации, участие и защита от насилия (социальное взаимодействие и полноправное включение, токсичная среда, возрастные ограничения и их проверка, защита от груминга и сексуальных злоупотреблений);
- право на конфиденциальность и свободу от экономической эксплуатации (бизнес модели предоставления доступа за данные, бесплатные игры и монетизация, отсутствие прозрачности в коммерческом контенте).

Передовой опыт: технология

The Google Virtual Reality Action Lab изучает, как виртуальная реальность может содействовать привлечению молодежи на сторону противников травли в реальной жизни и в онлайновой среде[1].

В сентябре 2019 года BBC запустила мобильное приложение, названное **Own IT** и посвященное благополучию детей в возрасте 8–13 лет, получивших свой первый смартфон. Приложение является частью обязательства BBC по поддержке молодых людей в современной меняющейся медийной среде и следующим шагом после успешного запуска веб-сайта Own IT в 2018 году. Приложение представляет собой сочетание современной технологии машинного обучения, отслеживающей действия ребенка на его смартфоне, с предоставленной ребенку возможностью самостоятельно отмечать свое эмоциональное состояние. В нем используется информация для предоставления индивидуально подобранного контента и вмешательства с тем, чтобы помочь ребенку оставаться счастливым и здоровым в онлайновой среде, предлагая дружественные и поддерживающие подсказки, когда их поведение выходит за рамки нормы. Пользователи могут обращаться к приложению в поисках помощи, при этом его также удобно использовать для выведения на экран мгновенных советов и подсказок при необходимости с помощью специально разработанной клавиатуры. В число функций приложения входят:

- напоминание пользователям подумать дважды, прежде чем делиться персональными данными, например номером мобильного телефона, в социальных сетях;
- помощь в понимании того, как сообщения могут восприниматься другими людьми, прежде чем отправлять их;
- отслеживание настроения во времени и советы о том, как изменить ситуацию при необходимости;
- предоставление информации по таким темам, как использование телефона поздно ночью и влияние на самочувствие пользователя.

[1] Более подробную информацию можно найти в публикации Alexa Hasse et al., "Youth and Cyberbullying: Another Look", Berkman Klein Center for Internet & Society, 2019.

В приложении используется специально подобранный контент из разных архивов BBC. В нем собраны полезные материалы и ресурсы, помогающие молодым людям извлечь максимум из времени, проведенного в онлайновой среде, и выработать здоровый стиль поведения и привычки работы в интернете. Оно помогает молодым людям и родителям вести более конструктивный разговор об их онлайновом опыте, не предоставляя отчетов или обратной связи родителям и сохраняя все данные исключительно на устройстве пользователя. Приложение не собирает никаких персональных данных или контента, созданного пользователем, поскольку весь процесс машинного обучения происходит внутри приложения, не покидая устройства, на котором оно установлено. Устройства обучаются обособленно на основе данных обучения, чтобы гарантировать отсутствие нарушений конфиденциальности.

2.1.3 Особая ситуация, в которой находятся дети-инвалиды[4]

Дети и молодые люди – инвалиды подвергаются рискам в онлайновой среде аналогично детям и молодым людям без инвалидности, однако они могут также подвергаться и конкретным рискам, обусловленным их инвалидностью. Они часто сталкиваются с отторжением, предрассудками и барьерами (физическими, экономическими, социальными и оценочными), препятствующими их участию в жизни сообществ. Такой опыт может оказывать негативное воздействие на ребенка-инвалида и вести к тому, что он начинает искать

[4] См. Council of Europe "Two clicks forward and one click back: report on children with disabilities in the digital environment", 2019.

социального взаимодействия и дружбы в онлайновом пространстве. Притом что такие взаимодействия могут положительно отражаться на формировании самооценки и создавать поддерживающие сети контактов, они также способны подвергать детей более высокому риску случаев груминга, склонения в онлайновой среде к действиям сексуального характера и/или сексуального домогательства. Согласно исследованиям, дети и молодые люди, имеющие сложности в реальном мире, а также испытывающие проблемы психологического характера, подвергаются повышенному риску подобных инцидентов[5] .

В целом, дети, которые становятся жертвами в реальном мире, вероятнее всего окажутся в том же положении в онлайновой среде. Это ставит детей-инвалидов под угрозу более высокого риска в интернете, притом что они испытывают большую потребность быть онлайн. Есть данные исследования, согласно которым дети-инвалиды с большей вероятностью подвергнутся насилию любого рода[6], в частности преследованиям сексуального характера[7]. Виктимизация может принимать форму травли, домогательства, изоляции и дискриминации по признаку реальной или мнимой инвалидности ребенка или же в связи с определенными особенностями, обусловленными его инвалидностью, – это могут быть особенности речи и поведения или оборудование или услуги, которыми он пользуется.

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[8]. 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.

Есть опасения в отношении того, что "шарентинг" (размещение родителями информации и фотографий своих детей и молодых людей в интернете) может нарушить право ребенка на неприкосновенность частной жизни, привести к травле и возникновению неловких ситуаций или негативно отразиться на дальнейшей жизни[9]. Некоторые родители детей-инвалидов могут делиться информацией или данными своих детей в поисках поддержки или совета, тем самым, ставя своего ребенка под угрозу нарушения конфиденциальности как в настоящем, так и в будущем. Такие родители также рискуют стать мишенью невежественных или беспринципных людей, предлагающих лечение или "исцеление" для их ребенка. В равной степени, некоторые родители детей или молодых людей – инвалидов могут проявлять гиперопеку в силу недостатка знаний о том, как лучше всего направлять своего ребенка при использовании интернета или как защитить его от травли или домогательства.[10]

5 Andrew Schrock et al., "Solicitation, Harassment, and Problematic Content", Berkman Center for Internet & Society, 2008.
6 UNICEF, "State of the World's Children Report: Children with Disabilities," 2013.
7 Katrin Mueller-Johnson et al., "Sexual Victimization of Youth with a Physical Disability: An Examination of Prevalence Rates, and Risk and Protective Factors", Journal of Interpersonal Violence, 2014.
8 Richard L Bruno, "Devotees, Pretenders and Wannabes: Two Cases of Factitious Disability Disorder", Sexuality and Disability, 1997.
9 UNICEF, "Child Privacy in the Age of Web 2.0 and 3.0: Challenges and opportunities for policy", Innocenti Discussion Paper 2017-03.
10 UNICEF, "Is there a ladder of children's online participation?", Innocenti Research Brief, 2019.

Некоторые дети и молодые люди – инвалиды могут сталкиваться с трудностями при использовании или даже отторжение от онлайновой среды ввиду недоступности ее структуры (например, приложения, которые не предусматривают возможности увеличения шрифта), отказом от запрошенных удобств (например, программ считывания с экрана или адаптивных средств управления) или необходимостью в приемлемой поддержке (например, обучение тому, как пользоваться оборудованием, индивидуальная поддержка по навигации при социальных взаимодействиях). [11]

2.2 Существующие национальные и транснациональные модели защиты ребенка в онлайновой среде

На глобальном уровне приняты несколько моделей сохранения безопасности детей и молодых людей в онлайновой среде. Заинтересованным сторонам в отрасли следует учитывать настоящие Руководящие указания в рамках международных инициатив, а также как основу обеспечения того, что они приложили все усилия для защиты детей и молодых людей в интернете. Интернет-отрасль – это разноплановая и запутанная сфера, состоящая из компаний разного размера и функций. Очень важно, чтобы защите детей уделяли внимание не только платформы и службы, занимающиеся контентом, но и те, кто поддерживает инфраструктуру интернета.

Необходимо отметить, что потенциал отрасли в плане введения всесторонней политики защиты детей ограничен имеющимися ресурсами. В связи с этим в настоящих Руководящих указаниях содержится рекомендация по объединению усилий разных отраслевых организаций для развертывания услуг по защите пользователей. Совместно используя ресурсы и технический опыт, они сумеют более эффективно создавать "безопасные пространства" в целях предотвращения насилия.

Отраслевое сотрудничество

Технологическая коалиция является примером успешного сотрудничества между заинтересованными сторонами в отрасли с целью борьбы с CSEA.

Транснациональные модели

Отраслевым организациям следует включать соответствующие международные руководящие указания в свои структурные программы, а также придерживаться всех соответствующих национальных и транснациональных законодательных норм, действующих в тех странах, в которых они работают. Им необходимо учитывать не только те действия, которые они обязаны предпринимать на установленном законом уровне, но и те действия, которые они могут выполнить, и, по мере возможности, стремиться к реализации инициатив по всему миру. В числе моделей, содержащих принципы для таких инициатив, можно назвать следующие:

- Правительственные Добровольные принципы противодействия CSEA в интернете пяти стран (2020 год);
- Комиссия по широкополосной связи в интересах устойчивого развития "Безопасность ребенка в онлайновой среде: снижение риска насилия, жестокого обращения и эксплуатации в онлайновой среде (2019 год)";
- Глобальный альянс WePROTECT "Глобальный стратегический ответ на сексуальную эксплуатацию и сексуальные злоупотребления в отношении детей в онлайновой среде" (2019 год);
- Глобальное партнерство по прекращению насилия в отношении детей "Учиться безопасно: призыв к действию";
- Достоинство ребенка в цифровом мире "Альянс за достоинство ребенка: отчет рабочей технологической группы (2018 год");

[11] Руководящие указания по таким правам представлены в Конвенции Организации Объединенных Наций о правах инвалидов и Факультативном протоколе к ней, в частности в статье 9 о доступности и статье 21 о свободе выражения мнения и убеждений и доступе к информации.

- Директива (ЕС) 2018/1808 Европейского Парламента и Совета Европейского Союза об аудиовизуальных медиа-услугах;
- Общий регламент Европейской комиссии о защите персональных данных (2018 год);
- Рекомендации ОЭСР по защите ребенка в онлайновой среде (2012 год).

Национальные модели

Существует целый ряд национальных и международных моделей, устанавливающих четкие роли и обязанности технологической отрасли в вопросах защиты детей в онлайновой среде. Некоторые из них не являются специфическими для детей как таковых, однако могут применяться к ним как к пользователям интернета. Они содержат всеохватные руководящие указания для отрасли в отношении регуляторной политики, стандартов и сотрудничества с другими секторами. В целях настоящего документа выделим ключевые принципы таких моделей в рамках их применения к отрасли ИКТ.

Кодекс проектирования с учетом возраста, Соединенное Королевство

В начале 2019 года Управление Комиссара по информации опубликовало предложения по кодексу проектирования с учетом возраста в целях защиты данных детей. Предлагаемый кодекс составлен исходя из лучших интересов ребенка, описанных в Конвенции ООН о правах ребенка, и устанавливает ряд требований к отрасли. Кодекс состоит из пятнадцати стандартов, в число которых входят отключение услуг определения местоположения по умолчанию для детей, сбор и хранение самого минимального количества персональных данных детей для отрасли, проектируемая конфиденциальность для продуктов, а также соответствующие возрасту и доступные объяснения.

Закон о вредоносной цифровой коммуникации, Новая Зеландия

Законом, принятым в 2015 году, злоупотребления в киберсреде выделены как отдельный вид преступления и рассматривается большой спектр типов наносимого вреда – от кибертравли до порнографии как мести. Он направлен на сдерживание, предотвращение и уменьшение цифровой коммуникации, являющейся вредоносной, делая незаконной публикацию цифровых материалов с намерением причинения серьезного эмоционального расстройства кому-то другому и устанавливая 10 принципов коммуникации. Закон создает возможности для подачи жалоб в независимую организацию в случае нарушения указанных принципов или для подачи судебного иска против автора или узла связи, если проблема не разрешается.

Комиссариат по электронной безопасности, Австралия

Учрежденный в 2015 году в Австралии Комиссариат по электронной безопасности является первым в мире государственным органом, учрежденным с целью решения вопросов злоупотреблений в интернете и обеспечения безопасности граждан в онлайновой среде. Будучи независимым национальным регулятором по вопросам безопасности в онлайновой среде, Комиссариат обладает полномочиями по целому ряду функций в диапазоне от профилактики (посредством повышения осведомленности, обучения, исследований и публикации руководящих указаний по передовым методам) до раннего вмешательства и устранения вреда посредством различных законодательных норм, дающих ему полномочия для быстрого пресечения кибертравли, злоупотреблений с использованием изображений и незаконного онлайнового контента. Столь широкий круг обязанностей обеспечивает Комиссариату возможность заниматься безопасностью в интернете на основе многогранного, целостного и упреждающего подхода.

В 2018 году Комиссариат по электронной безопасности разработал инициативу по проектируемой безопасности (Safety by Design, SbD), которая ставит безопасность и права пользователей в центр работы по проектированию, разработке и развертыванию онлайновых продуктов и услуг. Инициатива опирается на набор принципов проектирования, устанавливающих реалистичные, действенные и достижимые критерии для отрасли, обеспечивая более качественную защиту для граждан. Тремя всеобъемлющими принципами являются:

1) **Ответственность поставщика услуг**: груз обеспечения безопасности не должен целиком и полностью возлагаться на конечного пользователя. Уже на этапе проектирования можно выполнить ряд профилактических шагов, обеспечивающих оценку известного прогнозируемого вреда, и учесть их при предоставлении онлайновой услуги, наряду с шагами, снижающими вероятность того, что услуга будет способствовать, подталкивать или поощрять незаконные и неприемлемые действия.

2) **Предоставление прав и возможностей пользователю и его автономность**: достоинство пользователей и их лучшие интересы имеют первостепенную важность. Необходимо поддерживать выбор и автономность человека, подкрепляя и усиливая их за счет проектирования услуги, так чтобы дать пользователям возможность большего контроля, управления и регулирования их собственного опыта.

3) **Прозрачность и подотчетность**: это отличительные признаки надежного подхода к безопасности, который гарантирует, что услуги оказываются в соответствии с заявленными целями по безопасности, одновременно обучая и предоставляя общественности возможности в отношении шагов, которые можно предпринять для устранения проблем в данной области.

Глобальный альянс WePROTECT

В основе стратегии, принятой Глобальным альянсом WePROTECT, лежит поддержка стран при разработке скоординированных мер реагирования на случаи сексуальной эксплуатации детей в онлайновой среде в рамках предлагаемой Альянсом модели национального реагирования, которая служит проектом национальных программ. Стратегия дает странам схему, помогающую решить проблему сексуальной эксплуатации детей в онлайновой среде. В структуре модели национального реагирования WePROTECT выделяется четкий набор обязательств со стороны компаний сферы ИКТ в отношении:

- процедур уведомления и отключения;
- сообщения о сексуальной эксплуатации и сексуальных злоупотреблениях в отношении детей (CSEA) в онлайновой среде;
- разработки технологических решений; а также
- инвестирования в эффективные программы предотвращения СОР и службы реагирования.

Глобальное партнерство и фонд по прекращению насилия в отношении детей

Глобальное партнерство и фонд по прекращению насилия в отношении детей были учреждены Генеральным Секретарем ООН в 2016 году с единственной целью: активизировать и поддержать действия по прекращению всех форм насилия в отношении детей к 2030 году посредством уникального сотрудничества более чем 400 партнеров из всех секторов.

Проводимая работа ориентирована на спасение и поддержку жертв, технологические решения по выявлению и предотвращению преступлений, поддержку правоохранительных органов, проведение законодательных и политических реформ, а также на генерирование данных и доказательств о масштабах и характере CSEA в интернете и понимание ситуации с точки зрения детей[12].

[12] Руководящие указания по таким правам представлены в Конвенции Организации Объединенных Наций о правах инвалидов и Факультативном протоколе к ней, в частности в статье 9 о доступности и статье 21 о свободе выражения мнения и убеждений и доступе к информации.

3 Основные области в сфере защиты и содействия реализации прав детей

В этом разделе приводится описание **пяти основных вариантов действий** компаний в направлении обеспечения защиты детей и молодых людей при использовании ИКТ и содействия позитивному применению ИКТ.

3.1 Включение положений о правах ребенка во все соответствующие корпоративные политики и процессы управления

Необходимость учитывать права ребенка требует от компаний соответствующих мер по выявлению, предотвращению, смягчению и, по мере возможности, устранению потенциального или фактического негативного влияния на права ребенка. Руководящие принципы ООН по предпринимательской деятельности в аспекте прав человека призывают все предприятия и отрасли принять соответствующие политики и процедуры, направленные на исполнение их обязанности по уважению прав человека.

Отраслевым организациям следует уделять особое внимание детям и молодым людям как уязвимой группе в плане защиты их персональных данных и свободы выражения. Резолюция Генеральной Ассамблеи ООН 68/167 о праве на неприкосновенность личной жизни в цифровой век закрепляет право на неприкосновенность личной жизни и свободное выражение своего мнения без незаконного вмешательства. Кроме того, Резолюцией Совета по правам человека 32/13 о поощрении, защите и осуществлении прав человека в интернете признается глобальный и открытый характер интернета как одной из движущих сил ускорения прогресса по пути развития в его различных формах и подтверждается, что те же права, которые человек имеет в реальном мире, должны также защищаться и в онлайновой среде. В государствах с недостаточно определенными законодательными рамками в сфере защиты прав детей и молодых людей на личную жизнь и свободное выражение своего мнения компаниям следует придерживаться более строгих правил надлежащего исполнения, чтобы обеспечить соответствие своих политик и процедур международным законам. В связи с продолжающимся ростом участия молодежи в жизни гражданского общества посредством онлайновых коммуникаций компании несут ответственность по уважению прав детей и молодых людей даже в тех случаях, когда местное законодательство еще не доведено до уровня международных стандартов.

> Компаниям необходимо на оперативном уровне разработать механизм рассмотрения жалоб, определяющий формат постановки вопросов о потенциальных нарушениях лицами, подвергшимися негативному воздействию. Механизмы оперативного уровня должны быть доступными для детей, их семей и лиц, представляющих их интересы. Согласно разъяснениям, приведенным в Принципе 31 Руководящих принципов ООН по предпринимательской деятельности в аспекте прав человека, такие механизмы должны быть легитимными, доступными, предсказуемыми, справедливыми, транспарентными, соответствующими нормам в области прав человека, должны служить источником непрерывного обучения и быть основанными на взаимодействии и диалоге. Наряду с внутренними процессами контроля негативного влияния, механизмы рассмотрения жалоб должны гарантировать наличие в компаниях определенных рамок, обеспечивающих необходимые средства защиты прав детей и молодых людей в ситуациях, представляющих для них угрозу.

Стремясь к нормативному соответствию в области безопасности ИКТ, сфокусированному на соблюдении национального законодательства, следовании международным руководящим указаниям при отсутствии национальных законов и недопущении неблагоприятного влияния на права детей и молодежи, компании принимают упреждающие меры для содействия развитию и благополучию детей и молодых людей посредством проведения добровольных акций, направленных на содействие реализации прав ребенка на доступ к информации, свободное выражение своего мнения и участие, а также образовательных и культурных прав.

Передовой опыт: политика и проектирование с учетом возраста

Разработчик приложений Toca Boca изготавливает цифровые игрушки исходя из перспективы ребенка. Политика конфиденциальности компании составлена так, чтобы объяснить, какую информацию компания собирает и как ее использует. Toca Boca, Inc является членом Программы сертификации "безопасного пространства" PRIVO Kids Privacy Assured COPPA.

LEGO® Life служит примером безопасной платформы социальных сетей для детей моложе 13 лет, где они могут обмениваться своими поделками из LEGO, получать заряд вдохновения и безопасно взаимодействовать друг с другом. У детей не просят никакой персональной информации для создания учетной записи, для регистрации которой достаточно только адреса электронной почты родителя или опекуна. Приложение создает для детей и семей возможность обсудить вопросы безопасности и конфиденциальности в сети позитивно настроенной среде.

К примерам проектирования с учетом возраста относятся специальные предложения некоторых крупных компаний общественного вещания для определенных возрастных групп. Так в Германии ARD (Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland – Das Erste) и ZDF (Zweites Deutsches Fernsehen) нацелены на аудиторию детей от 14 лет, предлагая специально подобранный контент посредством онлайнового канала funk.net. BBC (British Broadcasting Corporation) запустила проект CBeebies, предназначенный для детей моложе 6 лет. Контент веб-сайта подобран специально для соответствующих возрастных групп.

Передовой опыт: политика и технологии

Twitter непрерывно инвестирует в собственные технологии, которые способствуют стабильному снятию с людей груза ответственности за сообщение о нарушениях[1]. В частности, более 50 процентов твитов (по сравнению с 20 процентами в 2018 году), которые Twitter отслеживает ввиду их оскорбительного характера, в настоящее время выявляются превентивно с помощью технологий, а не только полагаясь на сообщения, получаемые от пользователей. Новая технология используется в таких аспектах политики о контенте, как конфиденциальная информация, уязвимые средства передачи, действия, разжигающие ненависть, насилие и обезличивание.

[1] Twitter, "15th Transparency Report: Increase in proactive enforcement on accounts".

3.2 Разработка стандартных методов обращения со CSAM

В 2019 году IWF принял меры против 132 676 веб-страниц, содержащих подтвержденные материалы, связанные с сексуальными злоупотреблениями в отношении детей[13]. Любой URL может содержать сотни, если не тысячи изображений и видеоматериалов. Из всех изображений, блокированных IWF, 45 процентов представляли детей в возрасте 10 лет и моложе, и на 1609 веб-страницах демонстрировались дети в возрасте от 0 до 2 лет, причем 71 процент из них содержали сцены наиболее серьезных сексуальных злоупотреблений, таких как изнасилование и сексуальные пытки. Эти тревожные факты подчеркивают важность совместных действий между отраслями, правительственными и правоохранительными органами, а также гражданским обществом в плане борьбы со CSAM.

[13] IWF, "The why. The how. The who. And the results. Annual Report 2019".

В то время как правительства многих стран предпринимают активные действия по борьбе с распространением CSAM, усиливая законодательство, преследуя и наказывая правонарушителей, повышая уровень осведомленности и поддерживая детей и молодых людей в процессе их реабилитации после пережитого насилия или эксплуатации, многие страны пока еще не располагают приемлемыми системами. В каждой стране необходимы механизмы, с помощью которых широкая общественность может сообщать о такого рода контенте насильственного и эксплуатационного характера. Отрасль, правоохранительные и правительственные органы, а также гражданское общество, должны работать в тесном сотрудничестве, гарантируя надлежащие правовые рамки в соответствии с действующими международными стандартами. Такие рамки должны предусматривать уголовное преследование за все формы CSEA, в том числе посредством CSAM, защищать детей, ставших жертвами такого насилия или эксплуатации, а также обеспечивать максимально эффективное функционирование системы сообщения, расследования и удаления соответствующего контента.

Предприятия отрасли должны указывать на своих веб-сайтах ссылки на национальные горячие линии, такие как порталы IWF в некоторых странах и, при отсутствии местных возможностей для сообщения, указывать ссылки на другие соответствующие международные горячие линии, таки как в США Национальный центр по вопросам пропавших и эксплуатируемых детей (NCMEC) или Международная ассоциация горячих линий в интернете (INHOPE), через которую можно обратиться с сообщением на любую международную горячую линию.

Ответственные компании предпринимают целый ряд шагов по предупреждению ненадлежащего использования их сетей и услуг с целью распространения CSAM. В число таких шагов входит включение в принятые компаниями положения и условия или кодексы поведения пунктов, однозначно запрещающих подобный контент или действия[14], разработка действенных процессов уведомления и отключения, а также сотрудничество с национальными горячими линиями и поддержка их работы.

Кроме того, некоторые компании принимают технические меры по предотвращению ненадлежащего использования своих услуг и сетей для обмена известным CSAM. Например, некоторые поставщики услуг интернета также блокируют доступ к URL, на которых, согласно подтвержденным данным соответствующих органов, содержатся CSAM, если ведущий узел данного веб-сайта размещается на территории страны, где отсутствуют необходимые процессы, гарантирующие его быстрое удаление. Другие применяют технологии хэширования для автоматического выявления и удаления изображений, связанных с сексуальными злоупотреблениями в отношении детей, о которых правоохранительные органы или горячие линии уже получили информацию. Членам отрасли следует рассмотреть и внедрить в свою работу все соответствующие службы для предотвращения распространения сексуальных злоупотреблений в отношении детей.

Участникам отрасли необходимо дать обязательство по пропорциональному распределению ресурсов и продолжить разработку и обмен технологическими решениями предпочтительно с открытым кодом для выявления и удаления CSAM.

Передовой опыт: технология

Microsoft применяет четырехсторонний подход для содействия ответственному и безопасному использованию технологии с основным вниманием к технологии как таковой, самоуправлению, партнерствам, а также обучению и охвату потребителей. Компания Microsoft также внедрила функции, которые способствуют предоставлению отдельным людям возможности более эффективно управлять своей безопасностью в интернете. Одной из таких функций является "безопасность семьи", позволяющая родителям и опекунам контролировать использование интернета их ребенком.

[14] Необходимо отметить, что неприемлемое поведение пользователя не ограничивается исключительно CSAM, и компании должны соответствующим образом реагировать на любого рода неприемлемое поведение или контент.

На своих платформах Microsoft придерживается политики, направленной против домогательств, и учетные записи пользователей, которые нарушают это требование, закрываются или, в случае более серьезных нарушений, компания обращается в правоохранительные органы.

Microsoft PhotoDNA – это инструмент, создающий хэши изображений и сравнивающий их с базой данных хэшей, уже выявленных и подтвержденных CSAM. Если он находит совпадение, изображение блокируется. Этот инструмент дал поставщикам контента возможность удалить миллионы неправомерных фотографий из интернета, помог привлечь к ответственности сексуальных насильников над детьми и, в некоторых случаях, помог правоохранительным органам спасти потенциальных жертв до того, как им был нанесен физический вред. Microsoft уже давно следует обязательству защищать своих клиентов от незаконного контента в своих продуктах и услугах и применение технологии, уже разработанной компанией, для борьбы с ростом количества таких незаконных видеоматериалов стало логическим следующим шагом. Однако этот инструмент не использует технологию распознавания лица и не имеет возможности идентифицировать личность человека или объект по изображению. Тем не менее, с изобретением PhotoDNA for Video, ситуация получила новое направление развития. PhotoDNA for Video разбивает видеоролик на ключевые кадры и создает хэши для таких снимков экрана. Точно так же, как PhotoDNA умеет сопоставлять изображения, измененные во избежание обнаружения, PhotoDNA for Video способен находить контент с элементами сексуальной эксплуатации детей, подвергшийся редактированию или разделенный на ролики, которые в противном случае, казались бы безобидными.

Более того, недавно Microsoft выпустила новый инструмент для идентификации насильников над детьми, которые занимаются грумингом с целью злоупотреблений в онлайновых чатах. Проект Artemis, разработанный совместно с The Meet Group, Roblox, Kik и Thorn, основан на патентованной технологии Microsoft и будет выпущен в свободный доступ через Thorn для прошедших квалификацию компаний интернет-услуг, предлагающих функции чатов. Проект Artemis – это технологический инструмент, показывающий "красные флажки" администраторам при необходимости модерации в комнатах чата. Благодаря этому средству обнаружения груминга будет возможно идентифицировать, принимать меры и сообщать о преступниках, пытающихся соблазнить детей в сексуальных целях.

IWF предлагает ряд услуг для представителей отрасли, помогающих защитить их пользователей от контакта со CSAM. К ним, среди прочего, относятся:

- качественные динамичные списки блокирования URL, содержащих материалы прямых трансляций;
- списки хэшей известного криминального контента, связанного со CSAM;
- уникальные списки ключевых слов шифрованных понятий, которые, как известно, связаны со CSAM;
- список деталей доменных имен, под которыми, как известно, размещен контент, содержащий элементы сексуальных злоупотреблений в отношении детей, позволяющий быстро удалять домены, на которых размещен незаконный контент.

3.3 Создание более безопасной, соответствующей возрасту онлайновой среды

Крайне мало вещей в нашей жизни можно считать абсолютно безопасными и не несущими никакого риска. Даже в городах с максимально развитой системой регулирования дорожного движения все еще происходят аварии. Точно так же киберпространство не лишено рисков, особенно для детей и молодых людей. Дети и молодежь могут рассматриваться как получатели, участники и действующие лица в их онлайновом окружении. Риски, с которыми они сталкиваются, можно разбить на четыре категории[15]:

- *Неприемлемый контент* – дети и молодые люди могут сталкиваться с неприемлемым и незаконным контентом в процессе поиска других материалов, нажимая на предположительно невинную ссылку в полученном сообщении, блоге или при обмене файлами. Кроме того, дети могут искать неприемлемые или не соответствующие возрасту материалы и обмениваться ими. Представление о том, что следует считать вредоносным контентом, зависит от конкретной страны, при этом в число примеров входят материалы, поддерживающие злоупотребление запрещенными веществами, пропаганду расовой ненависти, рискового или суицидального поведения, анорексии или насилия.
- *Неприемлемое поведение* – дети и взрослые могут пользоваться интернетом с целью преследования или даже эксплуатации других людей. Дети иногда могут распространять обидные комментарии или задевающие чью-либо гордость изображения, а также могут воровать контент или нарушать авторские права.
- *Неприемлемый контакт* – как взрослые, так и молодые люди могут пользоваться интернетом с целью поиска уязвимых детей или других молодых людей. Часто их цель заключается в том, чтобы убедить объект поиска в формировании между ними значимых отношений, хотя в основе такой цели лежит стремление манипулировать своим контактом. Они могут стараться склонить ребенка к выполнению действий сексуального или иного оскорбительного характера в онлайновой среде с использованием веб-камеры или другого записывающего устройства, или же они могут предпринять попытку организовать личную встречу с физическим контактом. Такой процесс часто называют "грумингом".
- *Коммерческие риски* – в эту категорию входят риски, связанные с конфиденциальностью при сборе и использовании данных ребенка, а также с цифровым маркетингом. Безопасность в онлайновой среде – это вызов для общества и возможность для отрасли, правительства и гражданского общества благодаря совместным усилиям разработать соответствующие принципы и методы ее обеспечения. Отрасль может предложить целый ряд технических подходов, инструментов и услуг для партнеров, а также для детей и молодых людей и, прежде всего, должна создавать продукты, которые просты в использовании, спроектированы безопасно и соответствуют возрасту их основной категории пользователей. К дополнительным подходам можно отнести инструменты для разработки новых систем проверки возраста без нарушения прав ребенка на неприкосновенность частной жизни и доступ или установку ограничений по доступу к несоответствующему возрасту контенту для детей и молодых людей, а также ограничения доступа для людей, с которыми дети могут контактировать, или времени, в течение которого они могут выходить в интернет. И, самое главное, схемы "проектируемой безопасности"[16], учитывающие потребность в конфиденциальности в процессе инноваций и проектирования продукции. Безопасность детей и ответственное использование технологий должны быть тщательно проанализированы заранее, не откладывая их на потом.

Некоторые программы дают родителям возможность контролировать тексты и прочую информацию, которую получают и отсылают их дети и молодые люди. При использовании программ такого типа важно открыто обсудить это с ребенком, в противном случае он может воспринять такое поведение как "шпионство", подрывающее доверие в семье.

[15] Sonia Livingstone et al., "EU Kids Online: Final Report", London school of economics, 2009.
[16] eSafety Commissioner, Safety by Design Overview, 2019.

Для компаний одним из способов определения того, какого типа поведения придерживаются и взрослые, и дети, какие типы действий являются неприемлемыми, и какими могут быть их последствия, является разработка правил приемлемого использования. Четкие и прозрачные механизмы обратной связи должны быть доступными для пользователей, у которых есть сомнения в отношении контента и поведения. Более того, все сообщения требуют должного контроля со своевременным предоставлением сведений о статусе сообщения. Несмотря на то, что в компаниях могут применяться разные механизмы последующего контроля в зависимости от конкретного случая, важно установить четкие временные рамки ответа, предоставить информацию о принятом решении и предложить способ дальнейших действий, если пользователь не удовлетворен полученным ответом.

Передовой опыт: сообщения о проблемах

Facebook, стремясь к сдерживанию сексуальных домогательств на цифровых платформах, приняла участие в финансирование Проекта deSHAME в Европейском Союзе совместно с Childnet, Save the Children, Kek Vonal и UCLan. Этот проект направлен на активизацию сообщений о проблемах, связанных с сексуальными домогательствами в интернете, среди несовершеннолетних и расширение межотраслевого сотрудничества в целях предотвращения подобного поведения и реагирования на него.

Поскольку одной из главных целей проекта является поощрение пользователей к сообщению о контенте, который их расстраивает или является неприемлемым, с ним также можно соотнести Стандарты сообщества Facebook как руководящие указания о том, что разрешено, а что нет в Facebook. В них также определены типы пользователей, которым запрещено делать публикации. Facebook также разработала функции безопасности, например "Знаете ли вы этого человека?", ящик входящие сообщений "другие", в которой попадают новые сообщения от людей, не известных пользователю, и всплывающее окно, появляющееся в ленте новостей, если возникает подозрение в том, что к несовершеннолетнему обращается взрослый, которого данный ребенок не знает.

Поставщики онлайнового контента и услуг также могут приводить описание характера предоставляемых ими материалов и указывать возрастную группу, для которой они предназначены. Такие описания следует согласовывать с действующими национальными и международными стандартами, соответствующими нормами и рекомендациями по методам маркетинга и рекламы для детей, распространяемыми соответствующими классификационными органами. Тем не менее, данный процесс заметно осложняется ввиду растущего количества интерактивных услуг, допускающих публикацию созданного пользователями контента, например на электронных досках объявлений, в тематических чатах и социальных сетях. Если целевой аудиторией компании являются дети и молодые люди, или в случаях, когда услуги ориентированы, главным образом, на молодежь, ожидания в отношении **дружественного к пользователю, понятного и доступного контента** и безопасности будут значительно более высокими.

Кроме того, поощряется принятие компаниями самых строгих стандартов защиты конфиденциальности в ситуациях, требующих сбора, обработки и хранения данных, полученных от детей и молодых людей или касающихся их, поскольку дети и молодые люди могут быть недостаточно зрелыми, чтобы оценить широкие социальные и личные последствия раскрытия или согласия на предоставление их персональной информации в интернете или на использование их персональных данных в коммерческих целях. Услуги, направленные исключительно или главным образом на детскую и юношескую аудиторию, должны учитывать риски, которым они подвергаются в связи с доступом к таким услугам или сбором и использованием их персональных данных (включая сведения о местонахождении), и гарантировать соответствующие действия в связи с такими рисками и информирование пользователей. В частности, компании должны гарантировать, что язык и стиль всех материалов и информации, которые используются для продвижения услуг, предоставления доступа к услугам или для доступа к личной информации, ее сбора и использования, способствуют пониманию и помогают пользователям контролировать собственную конфиденциальность четкими и ясными способами, а также ясно и понятно разъясняют, на что именно соглашаются пользователи.

Передовой опыт: инновации

В 2018–2019 годах Региональное отделение для Восточной Азии и Тихого океана ЮНИСЕФ организовало пять круглых столов для многих заинтересованных сторон с целью обмена перспективным передовым опытом в области CSEA. Участниками круглых столов стали представители ведущих компаний частного сектора, такие как Google, Facebook, Microsoft, Telenor, Ericsson, MobiCom (Монголия), Mobifone+ (Вьетнам), Globe Telecom (Филиппины), True (Таиланд), Ассоциация GSM, а также партнеры, представляющие гражданское общество, в том числе INHOPE, ECPAT International и Международная линия помощи детям.

В части того же проекта в феврале 2020 года ЮНИСЕФ запустил "мозговой центр" для ускорения выхода отрасли на лидирующие позиции в Восточной Азии и Тихоокеанском регионе в целях предотвращения насилия против детей в онлайновом мире. Мозговой центр – это инкубатор идей и инноваций, основанный на уникальной перспективе участников отрасли (создание продуктов, маркетинг и пр.) в плане разработки результативных обучающих материалов и выявления наиболее эффективных платформ доставки, а также для разработки схем развития, позволяющих измерять воздействие таких обучающих материалов и сообщений, направленных на детей. В состав мозгового центра вошли специалисты Facebook, Telenor, эксперты академических организаций, учреждения ООН, такие как МСЭ, ЮНЕСКО и ЮНОДК, а также другие представители от таких организаций как Комиссариат по электронной безопасности Австралии, ECPAT International, ICMEC, Интерпол и Глобальный фонд по прекращению насилия в отношении детей. Мозговой центр созвал собрание, проведенное параллельно с Региональной конференцией АСЕАН по защите ребенка в онлайновой среде, собрав специалистов, в том числе из Microsoft, для изучения технологий и исследования возможностей для лучшего отслеживания изменений в онлайновом поведении на основании показателей использования материалов и сообщений по безопасности в онлайновой среде.

3.4 Обучение детей, опекунов и педагогов правилам детской безопасности и ответственного использования ими ИКТ

Технические меры могут быть важным средством обеспечения гарантии защиты детей и молодых людей от потенциальных рисков, с которыми они сталкиваются в онлайновой среде, но это только одна составляющая уравнения. **Инструменты родительского контроля, повышения осведомленности** и обучения также являются ключевым компонентом, способствующим расширению прав и возможностей и информированию детей и молодых людей различных возрастных групп, а также их родителей, опекунов и педагогов. Хотя компании играют важную роль в обеспечении ответственного и безопасного способа использования ИКТ детьми и молодыми людьми, родители, школа и сами дети и молодые люди разделяют с ними эту ответственность.

Многие компании инвестируют в образовательные программы, направленные на то, чтобы пользователи могли принимать информированные решения в отношении контента и услуг. Компании помогают родителям, опекунам и педагогам направлять детей и молодых людей в плане более безопасного, более ответственного и приемлемого поведения в онлайновой среде и в сетях подвижной телефонной связи. Такая работа включает маркировку классифицируемого по возрасту контента и четкое указание информации по таким вопросам, как стоимость контента, условия подписки и способы отмены подписки. Поддержка соблюдения требований по минимальному возрасту в социальных сетях во всех странах, где есть возможность проводить такую проверку, также поможет защитить детей, позволяя предоставлять им услуги доступа в приемлемом возрасте. Важным соображением, которое следует учитывать наряду с данной рекомендацией, является неизбежный сбор дополнительных данных для выполнения этого требования и необходимость ограничения сбора, хранения и обработки такой информации.

Также важно предоставлять информацию о более безопасном использовании ИКТ и позитивном и ответственном поведении непосредственно детям и молодым людям. Помимо повышения уровня осведомленности о безопасности, компании могут способствовать развитию позитивного опыта, разрабатывая контент для детей и молодых людей, информирующий о том, что, пользуясь ИКТ, необходимо вести себя уважительно, доброжелательно и открыто, а также следить за поведением своих друзей. Они могут предоставлять информацию о тех действиях, которые необходимо предпринять в случае негативного опыта, например травли или груминга в онлайновой среде, и которые упрощают уведомление о таких инцидентах и предоставляют возможность получения анонимных сообщений.

Родители иногда гораздо меньше разбираются в интернет-технологиях и мобильных устройствах, чем дети и молодые люди. Более того, совмещение мобильных устройств и интернет-услуг значительно усложняет возможности надзора со стороны родителей. Отрасль может сотрудничать с государственными и образовательными учреждениями с целью усиления возможностей родителей в плане поддержки их детей при формировании их собственной устойчивости к воздействию цифровой среды и моделей поведения, свойственных ответственным цифровым гражданам. Цель состоит не в том, чтобы перенести ответственность за использование ИКТ детьми только на родителей, а в признании того, что родители находятся в более выгодном положении при выборе приемлемого материала для своих детей и должны осознавать все риски, чтобы защитить их и дать им возможность действовать.

Информация может передаваться как различным каналам передачи информации как в сети, так и вне ее, принимая во внимание тот факт, что некоторые родители не пользуются интернетом. Важным является сотрудничество с отделами школьного образования в том, что касается включения тем безопасности в онлайновой среде и ответственного пользования ИКТ в учебный план для детей и молодых людей и образовательные материалы для родителей. В числе примеров можно назвать разъяснение того, какие доступны типы услуг и возможности для осуществления контроля, какие действия можно предпринять, если ребенок подвергается травле или грумингу в онлайновой среде, как избежать спама и регулировать настройки конфиденциальности, а также как разговаривать с мальчиками и девочками разных возрастов на деликатные темы. Общение – это двухсторонний процесс, и многие компании предоставляют своим клиентам возможность связаться с ними и сообщить о возникших проблемах или обсудить сомнения.

Поскольку объемы контента и услуг неизменно растут, рекомендации и напоминания о характере определенной услуги и о том, как безопасно ею пользоваться, будут оставаться полезными для всех пользователей. При всей важности обучения детей способам ответственного использования интернета, мы знаем, что дети любят экспериментировать, рисковать, обладают естественным любопытством и не всегда могут принимать лучшие решения. Предоставляя им шанс реализовать эту потребность, мы способствуем их росту и обеспечиваем здоровый способ развития самостоятельности и устойчивости к воздействиям до тех пор, пока последствия таких экспериментов не являются слишком жесткими. Притом что детям необходимо разрешать принимать определенный риск в онлайновой среде, крайне важно, чтобы родители и компании оказывали им поддержку в ситуациях, которые стали развиваться неправильно, смягчая негативное влияние неприятного опыта и превращая его в полезный урок на будущее.

Передовой опыт: образование

В Японии канал NHK проводит в Twitter кампанию по предотвращению самоубийств среди молодежи. Количество самоубийств достигает здесь пиковых показателей в период, когда дети возвращаются в школу после летних каникул. Причиной этому служит возврат в реальность. Продюсерская группа NHK Heart Net TV (NHK, Япония) выпускает мультимедийную программу #On the Night of August 31st. Объединив телевидение, прямое потоковое вещание и социальные сети, NHK успешно создал "место", где подростки могут поделиться своими чувствами, ничего не опасаясь.

Twitter также опубликовала руководство для педагогов по медийной грамотности. Составленный при поддержке ЮНЕСКО, этот учебник, прежде всего, предназначен в помощь преподавателям при формировании у молодых поколений навыков медийной грамотности. Еще один аспект работы Twitter в сфере безопасности связан с раскрытием информационных операций. Это архив поддерживаемых государством информационных операций, который Twitter предоставляет в открытый доступ. Инициатива была запущена с целью повышения в академической и общественной среде уровня понимания кампаний, связанных с данным вопросом, по всему миру и для обеспечения возможности независимого стороннего критического анализа данных тактик на платформе Twitter.

Проект deSHAME, финансируемый совместно Facebook и Европейским Союзом, также содействует созданию ресурсов для широкого спектра возрастных групп с особым акцентом на детях 9–13 лет. В рамках проекта был разработан набор инструментов "Step Up, Speak Up!", предлагающий ряд обучающих материалов для повышения осведомленности, а также практические инструменты для профилактической работы и стратегий реагирования в различных секторах. Обучающие материалы проекта будут передаваться в другие страны Европы и партнерам по всему миру в целях содействия пониманию своих цифровых прав среди молодежи.

Компания Google разработала ряд образовательных инициатив, ресурсов и инструментов для содействия повышению безопасности молодежи в онлайновой среде. Одной из них является кампания Be Internet Awesome, посвященная цифровому гражданству и разработанная в сотрудничестве с такими организациями, как ConnectSafely, Институт безопасности семьи в онлайновой среде и Internet Keep Safe Coalition. Эта кампания направлена на молодых людей в возрасте от 8 до 11 лет. Она содержит интернет-игру для молодежи (Interland), обучающую их основам цифровой безопасности и предоставляющую ресурсы для педагогов по таким темам, как цифровое гражданство и учебный план по вопросам безопасности. Учебный план по вопросам безопасности предлагает планы уроков по пяти основным тематическим областям кампании, одна из которых посвящена кибертравле. Помимо того, компания Google разработала онлайновый курс по цифровому гражданству и безопасности для педагогов, преподающих ученикам всех возрастов, предоставляя дальнейшую поддержку для проведения занятий по цифровому гражданству и мероприятий по безопасности в классах. Google также предлагает ряд программ для помощи непосредственно молодым людям в области безопасности в онлайновой среде и цифрового гражданства. Глобальная инициатива Web Rangers является одной из таких программ, которые обучают молодых людей безопасности в онлайновой среде и содействуют им в разработке собственных кампаний по позитивному и безопасному использованию интернета. Существуют также специализированные страновые программы для молодых людей, такие как Internet Citizens и Internet Legends в Соединенном Королевстве, запущенные Google.

В рамках **молодежного обмена новостями "Евровидение"**, Европейский радиовещательный союз объединяет 15 европейских телекомпаний, которые обмениваются программами, форматами и решениями в сети и за ее пределами. За последние годы обучение цифровой грамотности и предупреждение детей о рисках, в интернете стало основным в этих программах. Среди наиболее успешных инициатив последних лет можно назвать программы рекламы и новостей в социальных сетях, приемлемые для детей, выпускаемые Super и Ultra nytt на канале норвежской общественной радиовещательной организации NRK.

Передовой опыт: стратегические партнерства

В рамках проекта, поддерживаемого Глобальным фондом по прекращению насилия в отношении детей, в 2018 году Capital Humano y Social Alternativo заключил партнерское соглашение с Telefónica – крупнейшим поставщиком услуг интернета, кабельного вещания и телефонии из Перу, обслуживающим 14,4 миллиона клиентов, в том числе более 8 миллионов пользователей услуг подвижной связи Movistar.

В рамках этого плодотворного партнерства было проведено несколько мероприятий:

- **Виртуальный курс по защите ребенка в онлайновой среде** был разработан Telefónica при технической поддержке Capital Humano y Social Alternativo. Этот курс теперь открыт для общего доступа на веб-сайте Telefónica, и компания отслеживает количество человек, зарегистрировавшихся и успешно закончивших его. Министерство образования Перу согласилось разместить ссылку на этот курс на своем официальном веб-сайте.
- **Буклет по безопасности в интернете** был разработан Capital Humano y Social Alternativo и распространен Telefónica через более чем 300 центров продаж услуг подвижной связи компании с целью повышения осведомленности о безопасности в онлайновой среде и рисках, связанных с CSEA в интернете, среди клиентов Telefónica.
- **Интерактивная игра по CSEA в онлайновой среде** была разработана Telefónica при технической поддержке Capital Humano y Social Alternativo для того, чтобы клиенты могли играть в нее, ожидая своей очереди в точках продаж компании.

Вслед за успешным опытом сотрудничества с Telefónica, Capital Humano y Social Alternativo заключило партнерское соглашение с поставщиком услуг интернета и кабельного телевидения **Econocable**, обслуживающим клиентов в удаленных районах Перу и районах с низким уровнем дохода.

3.5 Содействие развитию цифровых технологий как средства усиления участия в жизни гражданского общества

Статья 13 Конвенции ООН о правах ребенка гласит: "Ребенок имеет право свободно выражать свое мнение; это право включает свободу искать, получать и передавать информацию и идеи любого рода, независимо от границ, в устной, письменной или печатной форме, в форме произведений искусства или с помощью других средств по выбору ребенка". Компании могут выразить свое уважение к гражданским и политическим правам детей, создав условия, в которых технологии и реализация законодательных и политических норм, разработанные с целью защиты детей и молодых людей от вреда в онлайновой среде, не имеют непредвиденных последствий, ведущих к подавлению их права на участие и выражение своего мнения или лишающих их доступа к информации, важной для их благополучия. В системах проверки возраста очень важно обеспечить отсутствие ущемления естественных потребностей определенных возрастных групп на доступ к контенту, соответствующему их развитию.

В то же время бизнес и отрасль могут поддерживать права детей и молодых людей, предлагая механизмы и инструменты, упрощающие их участие. Они могут сделать акцент на возможности интернета в плане упрощения позитивного участия в жизни гражданского общества, стимулирования социального прогресса и влияния на устойчивое развитие и жизнеспособность сообществ, например посредством участия в социальных кампаниях и кампаниях по защите окружающей среды, а также посредством обеспечения подотчетности всех ответственных лиц. Располагая правильными инструментами и информацией, дети и

молодые люди занимают более выгодное положение в плане доступа к возможностям здравоохранения, образования и трудоустройства, а также в плане выражения своего мнения и потребностей в школе, обществе и стране. Они получают возможности доступа к информации о своих правах и могут искать информацию по затрагивающим их лично вопросам, таким как их сексуальное здоровье или ответственность политиков и правительства.

Компании также могут вкладывать средства в создание онлайнового опыта, приемлемого для детей и молодых людей с их семьями. Они могут поддерживать развитие технологии и контента, поощряющего и дающего детям и молодым людям возможность учиться, творить и предлагать решения. Их продукция всегда должна разрабатываться исходя из принципа проектируемой безопасности.

Кроме того, компании могут принять упреждающие меры для поддержки прав детей и молодых людей путем проведения работы над устранением цифрового разрыва. Участие детей и молодых людей требует цифровой грамотности – способности понимать и умения взаимодействовать в цифровом мире. Без такой способности граждане не смогут участвовать во множестве социальных функций, перешедших в цифровую плоскость, включая подачу налоговых деклараций, поддержку политических кандидатов, подписание онлайновых петиций, регистрацию рождения детей или простой доступ к коммерческой, образовательной, культурной информации или информации, касающейся собственного здоровья. При общем бездействии пропасть между гражданами, способными пользоваться подобными форумами, и теми, у кого нет такой возможности ввиду отсутствия доступа к интернету или цифровой безграмотности, будет все больше расширяться, ставя последнюю группу во все более невыгодное положение. Компании могут поддерживать мультимедийные инициативы по развитию цифровых навыков, необходимых детям и молодым людям для того, чтобы чувствовать себя уверенно, ощущать свою причастность и проявлять активную позицию в жизни гражданского общества[17]. Во многих странах за последние годы повышение цифровой и медийной грамотности и усилия по устранению цифрового разрыва стали частью миссии общественных средств массовой информации. Так парламент Италии предложил национальным радиовещательным организациям поставить устранение цифрового разрыва и обеспечение защиты ребенка как в онлайновой среде, так и в реальном мире на одно из первых мест – пример, который следует перенять другим странам.

Передовой опыт: межучрежденческое сотрудничество

Недавно компания Microsoft присоединилась к глобальной кампании Power of ZERO, проводимой организацией No Bully с целью помощи детям и взрослым, заботящимся о них, научиться пользоваться цифровыми технологиями и выражать свое мнение, сочувствие и инклюзивность, составляющие основу цифрового гражданства. Инициатива предлагает педагогам, занимающимся с детьми младшего возраста (кампания направлена на детей моложе 8 лет), и семьям бесплатные учебные материалы в помощь при формировании "12 способностей добра" (выделенных Power of Zero 12 жизненно важных навыков или "способностей", позволяющих детям успешно ориентироваться как в онлайновой среде, так и реальном мире, включая навыки устойчивости, уважения, инклюзивности и творчества) и создании прочной основы, начиная с юного возраста.

[17] Примеры участия молодежи из сообщества подвижной связи можно найти здесь.

4 Общие руководящие указания для отрасли

В Таблице 1 представлены общие руководящие указания для отрасли по выявлению, предотвращению и смягчению любого рода неблагоприятного влияния продуктов и услуг на права детей и молодых людей, а также по содействию позитивному использованию ИКТ детьми и молодыми людьми.

Обратите внимание, что все шаги, перечисленные в Таблице 1, можно применить ко всем компаниям и услугам и они не являются обязательными шагами для каждой отдельной услуги, упомянутой в данной Таблице. Общие руководящие указания для отрасли дополняются контрольными перечнями по отдельным функциям (см. раздел 5) и наоборот. Контрольные перечни по отдельным функциям, представленные в Таблицах 2–5 освещают дополнительные шаги, наиболее приемлемые для отдельных услуг. Следует отметить, что контрольные перечни по отдельным функциям могут пересекаться в определенных аспектах и что одна и та же услуга может соотносится сразу с несколькими перечнями.

Таблица 1 – Общие руководящие указания для отрасли

Включение положений о правах ребенка во все соответствующие корпоративные политики и процессы управления	Отрасль может выявлять, предотвращать и ослаблять неблагоприятное влияние ИКТ на права детей и молодых людей, а также определять возможности для содействия реализации прав детей и молодых людей, предпринимая следующие действия:
	Назначить конкретное лицо и/или группу, ответственную за проведение данного процесса и имеющую доступ ко всем необходимым внутренним и внешним заинтересованным сторонам. Наделить такое лицо и/или группу полномочиями по управлению повышением профиля защиты ребенка в онлайновой среде в рамках компании.
	Разработать политику защиты и охраны детей и/или включить конкретные пункты о рисках и возможностях, связанных с правами детей и молодых людей, в документы, определяющие общекорпоративные обязательства (например, по правам человека, конфиденциальности, маркетингу или соответствующим кодексам поведения).
	Ввести процедуры надлежащего исполнения по вопросам СОР в существующие рамки обеспечения прав человека и оценки риска (например, на корпоративном уровне, на уровне продукции и технологий и/или на уровне страны) с целью выявления возможного оказания неблагоприятного влияния или способствования такому влиянию со стороны деятельности компании или отрасли или установления возможной прямой связи между неблагоприятным влиянием и действиями компании, ее продукцией, услугами или деловыми отношениями.
	Определить влияние на права ребенка в различных возрастных группах, обусловленное деятельностью компании, проектированием, разработкой и внедрением продукции и услуг, а также установить возможности по поддержке прав детей и молодых людей.
	Принять такой подход к защите ребенка, который основан на расширении прав и возможностей и обучении. Учитывать права детей на защиту данных, их права на конфиденциальность и свободу высказываний, в то же время предлагая обучение и инструкции по услугам компании. Опираясь на рекомендации внутренних и внешних экспертов и консультируясь с ключевыми заинтересованными лицами, в том числе с детьми и молодыми людьми, по вопросу механизмов обеспечения безопасности ребенка в онлайновой среде, установить способы получения постоянной обратной связи и инструкций по используемым компанией подходам.
	В государствах с недостаточно определенными законодательными рамками в сфере защиты прав детей и молодых людей на конфиденциальность и свободное выражение своего мнения компаниям следует придерживаться более строгих правил надлежащего исполнения, чтобы обеспечить соответствие своих политик и процедур международным стандартам. См. Резолюцию Генеральной Ассамблеи ООН 68/167 о праве на неприкосновенность личной жизни в цифровой век.
	Обеспечить доступ к средствам защиты, внедрив на оперативном уровне механизмы рассмотрения жалоб и обратной связи по всем случаям нарушений прав ребенка (например, по CSAM, неприемлемому контенту или контактам, вмешательствам в личную жизнь).

Включение положений о правах ребенка во все соответствующие корпоративные политики и процессы управления (*продолжение*)	Назначить менеджера по вопросам политики защиты детей или другое ответственное лицо, к которому можно будет обращаться в связи с проблемами СОР. Если ребенок находится под угрозой причинения ему вреда, менеджер по вопросам политики защиты детей должен незамедлительно уведомить соответствующие органы. Например, в редакторских руководящих указаниях BBC (2019 г.) указано, что назначение менеджера по вопросам политики защиты детей является обязательным в сфере общественных средств массовой информации.
Разработка отраслевых стандартов по защите детей в онлайновой среде	Создать и внедрить стандарты компании и отрасли по защите детей и молодых людей с учетом отраслевой специфики и характеристик.
Разработка стандартных методов обращения со CSAM	Совместно с государственными и правоохранительными органами, представителями гражданского общества и "горячих линий" отрасль играет важную роль в борьбе со CSAM, предпринимая следующие действия:
	Запретить загрузку, публикацию, передачу, обмен или предоставление открытого доступа к контенту, нарушающему права какой-либо из сторон или требования местного, регионального, национального или международного законодательства.
	Распространить среди национальных правоохранительных органов или национальных "горячих линий" информацию о передаче сообщений о CSAM незамедлительно, как только о них становится известно передающему. Обеспечить наличие внутренних процедур, направленных на выполнение предусмотренных местным и международным законодательством требований в отношении передачи таких сообщений. Если компания работает на рынке с менее развитой системой регуляторного и правоохранительного надзора в данной области, она может направлять свою информацию в Международную ассоциацию горячих линий в интернете (INHOPE), через которую можно передавать сообщения на любую международную горячую линию.
	Ввести внутренние процедуры, обеспечивающие соответствие местному и международному законодательству по борьбе со CSAM. Учредить высшую руководящую должность или отдел по внедрению таких процедур в структуре организации. После чего члены отрасли обязаны будут вносить сведения о предпринятых действиях и достигнутых результатах работы такого отдела в свои ежегодные корпоративные отчеты и отчеты по устойчивому развитию. При отсутствии достаточной защиты на уровне национальных законодательных норм, компании должны, соблюдая национальное законодательство, придерживаться более строгих требований и использовать собственные рычаги воздействия для лоббирования изменений в структуре законодательства, позволяющих отрасли эффективно бороться со CSAM. Необходимо учредить высшую руководящую должность или отдел в структуре организации по интегрированию таких процессов и контролю за их исполнением. Их работа должна быть прозрачно отражена в ежегодных корпоративных отчетах и отчете по устойчивому развитию, и соответствующая информация должна быть открыта для широкой общественности.
	Закрепить всестороннее сотрудничество с правоохранительными органами при расследовании случаев обнаружения или сообщения о незаконном контенте и определить детали соответствующих мер ответственности, например, штрафов или отмены льготной оплаты услуг.
	Использовать положения и условия для клиентов и/или соответствующие правила пользования, чтобы однозначно определить позицию компании в отношении неверного использования ее услуг с целью хранения или обмена CSAM и последствий подобных злоупотреблений.

Разработка стандартных методов обращения со CSAM (*продолжение*)	Разработать систему уведомления и отключения, а также процессы обратной связи, позволяющие пользователям сообщать о CSAM или неприемлемом контакте и указывать конкретный профиль/местоположение, где был обнаружен такой контент. Утвердить процессы последующего контроля сообщений, согласовать процедуры сбора доказательств и незамедлительного удаления или блокирования доступа к CSAM. Обеспечить, по мере необходимости, обращение поставщиков услуг за консультацией к специалистам (например, в национальные органы СОР) перед уничтожением незаконного контента. Убедиться, что соответствующие третьи лица, с которыми компания установила договорные отношения, применяют аналогичные надежные процедуры уведомления и отключения.
	Быть готовыми принимать меры в отношении CSAM и сообщать о них соответствующим органам власти. Если взаимоотношения между правоохранительными органами и национальной "горячей линией" еще не налажены, проводить с ними работу, направленную на совместную разработку соответствующих процессов.
	Работать с внутренними службами, в частности с отделом по работе с клиентами, отделом по профилактике мошенничества и службой охраны с целью обеспечения возможности сообщать о предполагаемых случаях незаконного контента непосредственно правоохранительным органам и на "горячие линии". В идеале, такая процедура не должна подвергать исполнительный персонал воздействию вредоносного контента, а также не должна способствовать повторному насилию над пострадавшим ребенком/пострадавшими детьми и молодыми людьми. В тех ситуациях, когда сотрудники могут подвергаться воздействию оскорбительного материала, установить правила или внедрить программу поддержки для восстановления их морального здоровья, безопасности и благополучия.
	Ввести правила удерживания и сохранения данных в целях оказания поддержки правоохранительным органам путем осуществления таких действий как сбор доказательств при расследовании уголовных дел. Документально оформить политики компании по обращению со CSAM, начиная с мониторинга и заканчивая окончательным переносом и уничтожением контента. Включить в состав документов перечень сотрудников, ответственных за выполнение различных операций с материалами.
	Содействовать внедрению механизмов обратной связи по CSAM и убедиться, что клиенты знают, как сообщить о факте обнаружения таких материалов. При наличии национальной горячей линии указать ссылки на нее на корпоративном веб-сайте и во всем соответствующем контенте, распространяемом компанией.
	Использовать все соответствующие службы/данные для предотвращения распространения известного контента, связанного с сексуальными злоупотреблениями в отношении детей, в рамках их услуг или платформ.
	Регулярно и активно проводить оценку всего контента, размещенного на серверах компании, включая коммерческий контент (как имеющий оригинальное фирменное содержание, так и полученный по договорам с третьими сторонами-поставщиками). Рассмотреть применение таких инструментов как сканирование хэш-индексов изображений, связанных с сексуальными злоупотреблениями в отношении детей, программ распознавания изображений или блокирования URL с целью принятия мер по обращению со CSAM.
Создание более безопасной, соответствующей возрасту онлайновой среды	Отрасль может оказать помощь в создании более безопасной, более увлекательной цифровой среды для детей и молодых людей всех возрастов, предпринимая следующие действия:
	Принять принципы безопасности и проектируемой конфиденциальности в технологиях и услугах компании и выделить как приоритетные те решения, которые позволяют снизить объем данных, связанных с детьми, до минимума.

Создание более безопасной, соответствующей возрасту онлайновой среды (*продолжение*)	Применять проектирование с учетом возраста в предлагаемых услугах. Представлять детям информацию о правилах сайта в доступной и соответствующей возрасту форме, указывая приемлемое количество подробностей. Помимо соответствующих возрасту и понятных положений и условий, предприятиям отрасли следует аналогичным образом в понятной форме сообщать различную информацию, такую как правила и ключевые политики. В них следует делать акцент на приемлемом и неприемлемом поведении в рамках услуги, последствиях нарушения правил, специфике услуги и том, на что пользователь дает согласие, регистрируясь в системе. Такая информация должна быть, в частности, ориентирована на юных пользователей и их родителей и опекунов.
	Использовать условия обслуживания или положения и условия для привлечения внимания пользователей к контенту в онлайновых услугах компании, которые могут быть приемлемыми не для всех возрастов. Положения и условия также должны определять четкие механизмы обратной связи и рассмотрения случаев нарушения установленных правил.
	Рассмотреть предоставление механизмов, например программ родительского контроля и других инструментов, дающих родителям и опекунам возможность управлять доступом детей к интернет-ресурсам, одновременно инструктируя их о правильном использовании таких средств во избежание нарушения прав детей. В их число входят черные/белые списки, фильтры контента, мониторинг использования, управление контактами и ограничение времени/программ.
	Предлагать простые в использовании инструменты родительского контроля, позволяющие родителям и опекунам ограничивать определенные услуги и контент, к которым дети могут иметь доступ с помощью электронных устройств. Такие ограничения могут охватывать управление на уровне сети и устройства, а также управление приложениями. Учитывая, что это оказывает огромное воздействие на способность ребенка развивать свои цифровые навыки и ухудшает их возможности в онайновой среде, такие средства управления следует разрабатывать для детей самого младшего возраста согласно уровню их развития и при условии правильного инструктирования родителей.
	По мере возможности содействовать развитию национальных служб поддержки, куда родители и опекуны могут сообщить о нарушениях и обратиться за помощью случаях насилия и эксплуатации.
	Избегать вредоносного или неприемлемого рекламного контента в интернете и установить обязательства по раскрытию клиентам информации об услугах, контент которых предназначен для взрослой аудитории и может оказаться вредным для детей и молодых людей. К числу вредоносной рекламы, в частности, можно отнести рекламу продуктов питания и напитков с высоким содержанием жиров, сахара или соли. Согласовать методы ведения бизнеса с нормами и рекомендациями по методам маркетинга и рекламы для детей и молодых людей. Контролировать, где, когда и как дети и молодые люди могут столкнуться с потенциально вредными рекламными сообщениями, предназначенными для другого сегмента рынка.
	Обеспечить соответствие политики сбора данных с действующими законами, затрагивающими личную жизнь детей и молодых людей, включая рассмотрение необходимости получения согласия родителей на сбор коммерческими предприятиями информации от ребенка или о нем.

Создание более безопасной, соответствующей возрасту онлайновой среды **(*продолжение*)**	Адаптировать и внедрить повышенные настройки конфиденциальности по умолчанию при сборе, обработке, хранении, продаже и публикации персональных данных, включая информацию о местоположении и наиболее частых просмотрах в интернете, касающихся лиц моложе 18 лет. Настройки конфиденциальности по умолчанию и информация о важности параметров конфиденциальности должны соответствовать возрасту пользователей и характеру услуги. Применять технические меры, например соответствующие инструменты родительского контроля, проектируемую конфиденциальность, разделение рабочей среды по возрастам с защитой контента паролями, черные/белые списки, контроль покупок/времени пользования, функции по согласию, фильтры и модерирование, чтобы предотвратить доступ малолетних детей и воздействие на них неприемлемого контента или услуг. Внедрять технологии, которые могут определять возраст пользователей и предлагать им соответствующую версию приложения. Для контента или услуг с возрастным цензом, заинтересованные стороны отрасли должны принимать меры по проверке возраста пользователей. По мере возможности использовать функции проверки возраста для ограничения доступа к контенту или материалам, которые согласно закону или политике компании предназначены только для лиц определенного возраста. Также компании должны признавать возможность неверного использования таких технологий с целью ограничения права детей и молодых людей на свободное выражение своего мнения и доступ к информации или угрозы их конфиденциальности.
	Обеспечить в отношении контента и услуг, которые по возрасту подходят не для всех пользователей: • классификацию согласно национальным стандартам и культурным нормам; • соответствие действующим стандартам в эквивалентных средствах информации; • четкое и хорошо видимое отображение с целью контроля доступа; • предложение, по мере возможности, одновременно с подтверждением возраста четких условий, касающихся удаления данных, идентифицирующих личность, получаемых в процессе такой проверки. Например, в отношении стандартов средств массой информации все регулирующие их деятельность органы предоставляют набор требований по связанному с возрастом контенту, и поставщики услуг интернета обязаны адаптировать свои хранилища данных и применять такие руководящие указания при предложении своего контента. См. требования Ofcom в Соединенном Королевстве, CSA во Франции и AGCOM в Италии.
	Предложить четкие инструменты обратной связи и разработать процесс последующего контроля сообщений о неприемлемом контенте, контакте или неверном использовании, а также предоставить пользователям услуги подробный отзыв о процессе обратной связи.
	Обеспечить предварительное модерирование интерактивных пространств для детей и молодых людей методами, согласующимися с правами детей на личную жизнь и их развивающимися возможностями. Активное модерирование может способствовать формированию атмосферы, в которой неприемлемы травля и домогательства. В число примеров неприемлемого поведения входят: • публикация неприятных или угрожающих комментариев к чьему-либо профилю; • создание подложных профилей или "сайтов ненависти" для унижения жертвы; • рассылка цепочек сообщений и вложений с намерением нанести вред; • взлом чужих учетных записей с целью отсылки оскорбительных сообщений другим.

Создание более безопасной, соответствующей возрасту онлайновой среды (***продолжение***)	Принять особые меры предосторожности в отношении штатных или нештатных сотрудников, которые работают с детьми и молодыми людьми и для которых может требоваться предварительная проверка их уголовного прошлого в правоохранительных органах.
	Незамедлительно передавать все предполагаемые случаи груминга на рассмотрение онлайновым или интерактивным группам исполнительного руководства, отвечающим за сообщение о них соответствующим органам: • сообщать, по мере возможности, о груминге в группу исполнительного руководства и назначенному менеджеру по вопросам защиты детей; • обеспечить пользователям возможность сообщать о предполагаемых случаях груминга непосредственно органам власти; • предоставить возможность для прямого контакта с целью предупреждения или сообщения через адреса электронной почты.
	В любых обстоятельствах считать безопасность и благополучие детей приоритетом своей работы. Всегда действовать в профессиональных рамках и обеспечить соответствие любого контакта с детьми действующей услуге, программе, событию, мероприятию или проекту. Никогда не брать единоличную ответственность за ребенка. Если ребенку необходима забота, предупредить об этом родителя, опекуна или сопровождающего. Всегда слушать и уважать детей. Если кто-то ведет себя неприемлемо в отношении детей, сообщить о таком поведении местному представителю по вопросами защиты детей.
	Установить четкий набор правил, которые размещаются на видном месте и, в целом, отражают важнейшие моменты положений и условий обслуживания и приемлемых руководящих указаний по использованию. Правила, составленные понятным для пользователя языком, должны определять: • характер услуги и ожидания в отношении ее пользователей; • что является и не является приемлемым с точки зрения контента, поведения и языка, а также запрет незаконного использования; • последствия соответственно степени допущенного нарушения, например, сообщение в правоохранительные органы или приостановление обслуживания учетной записи пользователя.
	Упростить для клиентов процесс сообщения о своих сомнениях в связи с неверным использованием контента сотрудникам отдела по работе с клиентами, установив стандартный и доступный порядок рассмотрения разного рода проблем, таких как получение нежелательных отправлений (например, SMS со спамом).
	Быть открытыми и предоставлять клиентам четкую информацию о характере предлагаемых услуг, например, о: • типе контента/услуги и стоимости; • минимальных возрастных требованиях для получения доступа; • наличии инструментов родительского контроля, включая указания о том, какие области охватывают (например, сеть) или не охватывают (например, Wi-Fi) такие средства контроля, и как научиться работать с ними; • типе собираемой информации о пользователе и характере ее использования.
	Содействовать развитию национальных служб поддержки, предоставляющих детям и молодым людям возможность сообщить или обратиться за помощью в случае, если они подвергаются насилию или эксплуатации (например, Международной линии помощи детям).

Обучение детей, родителей и педагогов правилам детской безопасности и ответственного использования ими ИКТ	Отрасль может дополнять технические меры действиями, направленными на повышение уровня образования и расширение прав и возможностей, предпринимая следующие действия:
	Четко описать доступный контент и соответствующие настройки родительского контроля или семейной безопасности. Используемый язык и терминология должны быть доступными, наглядными, понятными и значимыми для всех пользователей, включая детей, родителей и опекунов, особенно в том, что касается положений и условий, стоимости пользования контентом или услугами, политики конфиденциальности и механизмов обратной связи.
	Обучить клиентов тому, что следует делать в случае сомнений, связанных с использованием интернета, включая спам, кражу данных и неприемлемые контакты, например, травля и груминг, и описать, какие действия могут предпринять клиенты, и как им высказать свои сомнения о неприемлемом использовании.
	Установить механизмы и обучить родителей тому, как участвовать в связанных с ИКТ действиях детей и молодых людей, особенно в младшем возрасте, например предоставить родителям возможность проверять настройки конфиденциальности детей и молодых людей.
	Сотрудничать с государственными и образовательными органами в плане формирования родительского потенциала по поддержке детей и молодых людей и проведения с ними бесед на тему необходимости быть ответственными гражданами цифрового общества и пользователями ИКТ.
	Исходя из местного контекста предоставить материалы для школьного и домашнего использования, направленные на повышение качества использования ИКТ детьми и молодыми людьми и развитие у них критического мышления, позволяющего действовать безопасно и ответственно при пользовании услугами ИКТ.
	Поддерживать клиентов посредством распространения доступных инструкций по безопасности семьи в онлайновой среде, поощряя родителей и опекунов: • знакомиться с продуктами и услугами, которыми пользуются дети и молодые люди; • обеспечивать умеренное использование электронных устройств детьми и молодыми людьми, заботясь об их здоровом и сбалансированном образе жизни; • уделять пристальное внимание поведению детей и молодых людей, чтобы своевременно выявлять изменения, которые могут указывать на кибертравлю или домогательства в отношении них.
	Предоставить родителям необходимую информацию, помогающую понять, как дети и молодые люди пользуются услугами ИКТ, как урегулировать вопросы, связанные с вредоносным контентом и поведением, и как направить детей и молодых людей в русло ответственного использования. Эту задачу можно упростить за счет использования инструментов и благодаря взаимодействию с отделами школьного образования в области разработки учебных программ по безопасности в онлайновой среде и образовательных материалов для родителей.
Использование технологических достижений для защиты и обучения детей	Средства ИИ для сохранения конфиденциальности, которые распознают тексты, изображения, разговоры и контекст, способны выявить и принять меры в отношении целого ряда вредоносных ситуаций и угроз в интернете, используя эту информацию для расширения возможностей и обучения детей правилам действий в таких ситуациях. При выполнении в среде умного устройства это может защитить данные и конфиденциальность молодых людей, одновременно оказывая им поддержку.
	Общественные услуги и национальные средства массовой информации могут играть важную роль благодаря предлагаемым ими программам (в реальном мире и в онлайновой среде) по обучению родителей и детей и доведению до их сведения рисков и возможностей онлайнового мира.

Содействие продвижению цифровых технологий как средства усиления участия в жизни гражданского общества	Отрасль может поощрять детей и молодых людей и предоставлять им соответствующие возможности, поддерживая их право на участие, предпринимая следующие действия:
	Предоставить информацию об услуге, подчеркивая преимущества, которые дети могут получить, если будут вести себя правильно и ответственно, например, будут использовать услугу в творческих целях.
	Разработать письменные процедуры, гарантирующие последовательное внедрение политик и процедур, защищающих свободное выражение своего мнения для всех пользователей, включая детей и молодых людей, а также документацию в соответствии с этими политиками.
	Избегать чрезмерного блокирования законного и соответствующим образом разработанного контента. Чтобы не допустить неверного использования запросов и инструментов фильтрации для ограничения доступа детей и молодых людей к информации, обеспечить прозрачность информации о заблокированном контенте и установить для пользователей порядок сообщения о случайном блокировании. Такой порядок должен быть доступным для всех потребителей, включая администраторов сайтов. Все процедуры обратной связи должны обеспечивать установление четких, ответственных и признанных условий обслуживания.
	Разработать онлайновые платформы, способствующие реализации прав детей и молодых людей на выражение своего мнения, упростить их участие в общественной жизни и поощрять сотрудничество, предпринимательство и гражданское участие.
	Разработать образовательный контент для детей и молодых людей, поощряющий учиться, творить, думать и решать задачи.
	Содействовать повышению цифровой грамотности, созданию потенциала и развитию навыков ИКТ у детей и молодых людей, особенно у детей в сельских и недостаточно обслуживаемых районах, чтобы способствовать использованию ресурсов ИКТ и полноценному безопасному участию в цифровом мире.
	Сотрудничать с местным гражданским обществом и государственными органами по вопросам национальных и местных приоритетов в сфере расширения универсального и равноправного доступа к ИКТ, платформам и устройствам, включая лежащую в их основе инфраструктуру.
	Информировать клиентов, включая родителей, опекунов, детей и молодых людей, о предлагаемых услугах, вовлекая их в работу с ними, например сообщать о: • типе контента и соответствующих инструментах родительского контроля; • механизмах обратной связи в случаях проявления насилия, неправомерного использования и неприемлемого или незаконного контента; • процедурах последующего контроля сообщений; • типах услуг с возрастными ограничениями; • безопасном и ответственном использовании "собственных" интерактивных услуг компании.
	Заниматься вопросами более широкого плана в связи с безопасным и ответственным цифровым гражданством, например вопросами репутации в онлайновой среде и цифровой географии, вредоносного контента и груминга. Рассмотреть возможность партнерских взаимоотношений с экспертами местного уровня, в частности с НГО, благотворительными организациями и воспитательными группами, которые способны помочь при разработке обращений и рассылок компании и охвате целевой аудитории.
	Если компания уже работает с детьми или школами, например в рамках корпоративных программ социальной ответственности, выяснить, можно ли расширить такую деятельность, включив в нее обучение детей и молодых людей, а также **педагогов** методам СОР.
Инвестиции в исследования	Инвестировать в основанные на доказательствах исследования и углубленный анализ цифровых технологий, воздействия технологий на детей, защиты детей и прав ребенка в отношении цифрового окружения, с тем чтобы интегрировать онлайновые системы защиты в услуги, используемые детьми и молодыми людьми и лучше понять, какие типы вмешательства являются наиболее эффективными с точки зрения улучшения детского опыта в интернете.

Типология компаний ИКТ

Притом что настоящие Руководящие указания МСЭ предназначены для отрасли ИКТ в целом, важно признать, что услуги, предлагаемые компаниями ИКТ, способы осуществления их деятельности, регуляторные схемы, в рамках которых они функционируют, и объем и масштабы предложения значительно различаются. Все технологические компании, чьи продукты и услуги направлены прямо или косвенно на детей, могут извлечь пользу из общих принципов, изложенных выше, адаптируя их в зависимости от своей конкретной области деятельности. Основная идея заключается в поддержке и направлении отрасли ИКТ в плане принятия правильных мер для улучшения защиты детей в онлайновой среде от рисков нанесения вреда, одновременно наделяя их правами и возможностями для навигации по миру интернета наиболее приемлемыми способами. Приведенная ниже типология поможет лучше понять некоторые целевые аудитории и то, как они соотносятся с контрольными перечнями, размещенными в следующем разделе. Необходимо отметить, что это лишь некоторые конкретные примеры категорий, перечень которых не является исчерпывающим:

a) поставщики услуг интернета, в том числе услуг фиксированных наземных широкополосных сетей или услуг передачи данных по сотовым сетям операторов подвижной связи: притом что, как правило, такие услуги предлагаются на относительно долгосрочной основе по абонентским соглашениям, они также могут распространяться на компании, предоставляющие услуги бесплатных или оплачиваемых общественных точек доступа Wi-Fi;

b) социальные сети/платформы обмена сообщениями и онлайновых игр;

c) изготовители аппаратного и программного обеспечения, например поставщики портативных устройств, включая мобильные телефоны, игровые консоли, бытовые приборы с голосовыми помощниками, детские игрушки со встроенными устройствами интернета вещей и умного соединения с интернетом.

d) компании, предоставляющие цифровые средства (создающие или размещающие контент, предоставляющие доступ);

e) компании, предоставляющие услуги потоковой передачи данных, включая прямое потоковое вещание;

f) компании, предлагающие услуги цифрового хранилища файлов, поставщики облачных услуг.

5 Контрольные перечни по отдельным функциям

В этой главе приведенный ранее общий контрольный перечень для отрасли дополняется рекомендациями по уважению и поддержке прав ребенка в онлайновой среде для компаний, оказывающих услуги с определенными функциями. В следующих контрольных перечнях по отдельным функциям определены средства, дополняющие общие принципы и подходы, представленные в Таблице 1, в их привязке к различным услугам. Поэтому их следует считать дополнением к действиям, перечисленным в Таблице 1.

Представленные здесь функции накладываются друг на друга, и может быть так, что к одной и той же компании применяются сразу несколько перечней.

Следующие перечни по функциям организованы по тем же основным областям, что и общие руководящие указания в Таблице 1. Каждый из контрольных перечней по функциям разработан в сотрудничестве с основными соавторами, в связи с чем в таблицах отмечаются лишь незначительные вариации.

5.1 Функция A: предоставление услуг установления соединений, хранения и размещения данных

Доступ в интернет является основой реализации прав детей, и возможность установления соединений может отрыть для ребенка целый мир. Поставщики услуг установления соединений, хранения и размещения данных располагают огромными возможностями по обеспечению безопасности и конфиденциальности в рамках своих предложений для детей и молодых людей. Услуги данной категории охватывают, среди прочего, операторов подвижной связи, поставщиков услуг интернета, системы хранения данных и службы размещения данных.

Операторы подвижной связи предоставляют доступ в интернет и целый ряд услуг, связанных с подвижными технологиями передачи данных. Многие операторы уже утвердили кодексы СОР и предлагают целый ряд инструментов и информационных ресурсов в поддержку исполнения своих обязательств.

Большинство поставщиков услуг интернета выступают одновременно в роли посредников, предоставляющих доступ к интернету и из интернета, и репозитория, предоставляющего услуги ведущего узла, а также услуги по кэшированию и хранению данных. В результате они несут основную ответственность в плане защиты детей в онлайновой среде.

Доступ к интернету в общественных местах

Все чаще муниципальные службы, розничные предприятия, транспортные компании, сетевые отели и прочие коммерческие предприятия и организации предоставляют доступ к интернету с помощью беспроводных точек доступа Wi-Fi. Такой доступ обычно предоставляется бесплатно или за незначительную плату и иногда с минимальными требованиями по регистрации и используется общественными организациями или компаниями для привлечения клиентов в свои помещения или для убеждения большего количества людей пользоваться их услугами.

Продвижение Wi-Fi – это эффективный способ обеспечения доступности интернета в определенном регионе. Тем не менее, в общественных местах, которые часто посещаются детьми, следует принимать определенные меры предосторожности. Пользователи должны помнить, что сигналы Wi-Fi могут быть открытыми для всех проходящих мимо, подвергая риску их личные данные. Таким образом, поставщики услуг Wi-Fi не всегда имеют возможность поддерживать или контролировать использование предоставляемого ими интернет-соединения, и пользователям самим необходимо принимать меры во избежание обмена важной информацией через общедоступные точки Wi-Fi.

Поставщики услуг Wi-Fi в общественных местах могут рассмотреть возможность применения дополнительных мер защиты детей и молодых людей, в частности:

- помимо усилий по блокированию доступа к CSAM, принимать упреждающие меры с целью блокирования доступа к веб-адресам, которые, согласно имеющейся информации, содержат контент, неприемлемый для широкой аудитории;
- включить в положения и условия обслуживания пункты, запрещающие использование услуги Wi-Fi для доступа или демонстрации материалов, которые могут быть неприемлемыми в среде, где присутствуют дети. Положения и условия также должны определять четкие механизмы действия по ликвидации последствий нарушения таких правил;
- принять все меры по защите от несанкционированного доступа, который может привести к манипуляциям или утере персональных данных;
- установить фильтры в системе Wi-Fi, чтобы усилить действие правил в отношении неприемлемых материалов;
- разработать процедуры и программное обеспечения для обозначения и предложения дополнительных инструментов родительского контроля в связи с доступом детей и молодых людей к контенту в интернете.

Передовой опыт: Система регулирования электросвязи во многих странах – членах Европейского Союза, например, предусматривает, что доступ к сетям должен идентифицироваться посредством отдельной SIM-карты или других инструментов идентификации.

В Таблице 2 приводятся руководящие указания для поставщиков услуг установления соединений, хранения и размещения данных в отношении действий, направленных на повышение защиты и участия ребенка в онлайновой среде.

Таблица 2 – Контрольный перечень по COP для функции A: предоставление услуг установления соединений, хранения и размещения данных

Включение положений о правах ребенка во все соответствующие корпоративные политики и процессы управления	Поставщики услуг установления соединений, хранения и размещения данных могут выявлять, предотвращать и ослаблять неблагоприятное влияние ИКТ на права детей и молодых людей, а также определять возможности для содействия реализации прав детей и молодых людей.
	См. общие руководящие указания в Таблице 1.
Разработка стандартных методов обращения со CSAM	Совместно с государственными и правоохранительными органами, представителями гражданского общества и горячих линий поставщики услуг установления соединений, хранения и размещения данных могут играть важную роль в борьбе со CSAM, предпринимая следующие действия:
	Сотрудничать с государственными и правоохранительными органами, представителями гражданского общества и горячими линиями с целью эффективного урегулирования вопросов, вызванных CSAM, и сообщения о фактах их появления соответствующим органам. Если взаимоотношения между правоохранительными органами и горячей линией еще не налажены, проводить с ними работу, направленную на совместную разработку соответствующих процессов. Поставщики услуг установления соединений, хранения и размещения данных также могут проводить обучение по ИКТ для правоохранительных органов. Если компания работает на рынке с менее развитой системой регуляторного и правоохранительного надзора в данной области, она может направлять свою информацию Международной ассоциации горячих линий в интернете (INHOPE), через которую можно передавать сообщения на любую международную горячую линию.
	Рассмотреть возможность применения признанных на международном уровне черных списков URL или веб-сайтов, составленных соответствующими органами (например, национальными правоохранительными органами или горячими линиями, Cybertip Canada, Интерполом, IWF), чтобы усложнить пользователям доступ к уже установленным CSAM.
	Разработать процессы уведомления, отключения и сообщения и связать сообщения о злоупотреблении с этими процессами согласно открытому соглашению о процедурах реагирования и времени отключения контента. См., например, Руководство ЮНИСЕФ и Ассоциации GSM по политикам и методам уведомления и отключения.
	Установить механизм обратной связи с четкими инструкциями по его использованию, например предоставить инструкции по незаконному контенту и поведению, о которых необходимо сообщать, и разъяснять, какие материалы нельзя прилагать к сообщению, чтобы не допустить их дальнейшего распространения в сети.
	Оказывать поддержку правоохранительным органам при проведении уголовных расследований путем осуществления таких действий, как сбор доказательств. Установить в положениях и условиях обслуживания запрет на использование услуг для хранения/обмена или распространения CSAM. Убедиться, что в таких положениях ясно определена абсолютная неприемлемость CSAM. Четко указать в положениях и условиях обслуживания, что компания будет полностью сотрудничать с правоохранительными органами при проведении расследований в случае обнаружения CSAM или сообщения о нем.
	В настоящее время существует два решения для обратной связи по онлайновым CSAM на национальном уровне: горячие линии и порталы сообщений. Полный актуальный перечень всех действующих горячих линий и порталов можно найти на сайте INHOPE.

Разработка стандартных методов обращения со CSAM (*продолжение*)	Горячие линии: При отсутствии национальной горячей линии, рассмотреть возможности для ее организации. Всю информацию о вариантах можно найти в Практическом руководстве Ассоциации GSM по горячим линиям INHOPE, включая сотрудничество с INHOPE и Фондом INHOPE. Есть также интерактивная версия руководства Ассоциации GSM INHOPE, в котором приводятся инструкции о том, как разработать внутренние процессы для персонала службы поддержки клиентов по направлению сообщений о сомнительном контенте в правоохранительные органы и INHOPE.
	Порталы сообщений: IWF предлагает решение, которое дает возможность пользователям интернета в странах и государствах, не имеющих собственных горячих линий, сообщать об изображениях и видеоматериалах, которые могут быть связаны с сексуальными злоупотреблениями в отношении детей, в IWF через специализированную страницу онлайнового портала.
	Поставщикам услуг установления соединений, хранения и размещения данных, чьи услуги предполагают размещение определенного типа контента (многих это не касается), необходимо принять процессы уведомления и отключения.
Создание более безопасной, соответствующей возрасту цифровой среды	Поставщики услуг установления соединений, хранения и размещения данных могут оказать помощь в создании более безопасной, более увлекательной цифровой среды для детей разных возрастов, предпринимая следующие действия:
	Поставщики услуг хранения/размещения данных должны рассмотреть возможность предоставления функции обратной связи на всех страницах сайта и в рамках соответствующих услуг и разработать и оформить документально четкие процессы быстрой обработки сообщений о злоупотреблениях или других нарушениях положений и условий.
	Поставщики услуг установления соединений должны предлагать собственные технические средства контроля и обозначения действующих инструментов, которые созданы специализированными поставщиками, соответствуют предлагаемым услугам и удобны для пользователей, а также предлагать возможность блокирования или фильтрации доступа к интернету через сети компании. Установить приемлемые механизмы проверки возраста, если компания предлагает контент или услуги (включая собственные услуги или услуги третьих сторон, рекламируемые компанией), которые являются правомерными или приемлемыми только для взрослых пользователей (например, определенные виды игр, лотереи).
Обучение детей, родителей и педагогов правилам детской безопасности и ответственного использования ими ИКТ	Поставщики услуг установления соединений, хранения и размещения данных должны дублировать основные моменты своих положений и условий в руководящих указаниях для сообщества, написанных понятным пользователям языком, в целях поддержки детей и их родителей или опекунов. В рамках самой услуги в месте загрузки контента разместить напоминания о том, какие типы контента могут считаться неприемлемыми.
	Обеспечить детей и молодых людей информацией по более безопасному использованию интернета. Творчески подходить к распространению ключевой информации, пользуясь, например, следующими формулировками: "Никогда не давай контактную информацию, включая сведения о своем физическом местоположении и свой телефонный номер, людям, которых ты лично не знаешь". "Никогда не соглашайся на встречу с человеком, с которым ты знакомишься в интернете, предварительно не посоветовавшись со взрослым. Обязательно скажи своему другу, которому ты доверяешь, куда ты идешь". "Не отвечай на запугивающие, непристойные или оскорбительные сообщения, но сохрани доказательство – не удаляй такие сообщения". "Если ты испытываешь тревогу или тебе неловко из-за чего-то или кого-то, расскажи об этом взрослому или другу, которому доверяешь". "Никогда никому не называй свой пароль к учетной записи или имя пользователя! Знай, что другие люди в интернете могут жульничать, чтобы убедить тебя поделиться своей персональной информацией".

Обучение детей, родителей и педагогов правилам детской безопасности и ответственного использования ими ИКТ (*продолжение*)	Поставщики услуг могут объединять усилия с организациями, имеющими необходимые ресурсы для обучения и поддержки детей в плане более безопасного использования интернета и других взаимосвязанных вопросов. Примеры см. в практическом руководстве Международной линии помощи детям и Ассоциации GSM для горячих линий помощи детям и операторов подвижной связи: совместная работа ради защиты прав детей.
Содействие продвижению цифровых технологий как средства усиления участия в жизни гражданского общества	*См. общие руководящие указания в Таблице 1.*

5.2 Функция B: предложение отобранного цифрового контента

Интернет предлагает самые разные варианты контента и деятельности, многие из которых предназначены для детей и молодых людей. Компании, предоставляющие специально подобранный контент, располагают огромными возможностями по обеспечению безопасности и конфиденциальности в рамках своих предложений для детей и молодых людей.

В эту категорию входят как компании, создающие собственный контент, так и те, кто обеспечивает доступ к цифровому контенту. Ее составляют, среди прочего, услуги новостей и мультимедийного потокового вещания, национальные и общественные радиовещательные организации, а также представители игровой отрасли.

В Таблице 3 приводятся руководящие указания для компаний, предлагающих специально подобранный контент, в отношении политик и действий, направленных на повышение защиты и участия ребенка в онлайновой среде.

Таблица 3 – Контрольный перечень по СОР для функции B: предложение отобранного цифрового контента

Включение положений о правах ребенка во все соответствующие корпоративные политики и процессы управления	Компании, предлагающие специально подобранный контент, могут выявлять, предотвращать и ослаблять неблагоприятное влияние ИКТ на права детей и молодых людей, а также определять возможности для содействия реализации прав детей и молодых людей, предпринимая следующие действия:
	Разработать политики, оберегающие благополучие детей и молодых людей, пополняющих онлайновый контент, учитывая физическое и эмоциональное благополучие и достоинство молодых людей моложе 18 лет, принимающих участие в программах, фильмах, играх, новостях и пр. независимо от согласия, которое может предоставляться родителем или другим взрослым.
Разработка стандартных методов обращения со CSAM	Совместно с государственными и правоохранительными органами, представителями гражданского общества и горячих линий компании, предлагающие специально подобранный контент, могут играть важную роль в борьбе со CSAM, предпринимая следующие действия: В случаях CSAM, передаваемых, например, через функции "комментариев" или "обзоров", в которых пользователи могут выгружать свой контент, персонал должен связываться с исполнительным руководством, отвечающим за сообщение о таких материалах в соответствующие органы. Кроме того, необходимо: • незамедлительно уведомить национальные правоохранительные органы; • уведомить своего руководителя и сообщить о таких материалах менеджеру по вопросам политики защиты детей; • обратиться в службу внутренних расследований по телефону или электронной почте, указав подробности инцидента и попросив совета; • дождаться рекомендаций соответствующего органа прежде чем удалять материал, сохранять его в среде, открытой для общего доступа, или пересылать его.

Разработка стандартных методов обращения со CSAM (*продолжение*)	Если материал идентифицирован, о нем необходимо сообщить непосредственно в организацию, специализирующуюся в вопросах безопасности в интернете и обслуживающую систему обратной связи горячей линии, куда члены общественных организаций и профессионалы в области информационных технологий могут сообщать об особых формах потенциально незаконного онлайнового контента. Так, например, на основе своей Политики защиты и охраны интересов детей компания BBC выпустила редакторские руководящие указания по взаимодействию с детьми и молодыми людьми в интернете. Компания также разработала контрольные перечни и кодексы поведения при работе с детьми и молодыми людьми в интернете, которые, в том числе, распространяются на субподрядчиков и внешних поставщиков. В политике Ofcom в отношении защиты детей для Соединенного Королевства вопросы онлайнового контента, мобильных устройств и игровых консолей рассматриваются отдельно. Внедрить стратегию быстрой и надежной передачи дела по инстанциям в случаях, касающихся публикации CSAM или незаконного поведения. В этой связи: • предложить пользователям простой и доступный способ предупреждения изготовителя контента о нарушении каких-либо правил в онлайновом сообществе; • удалять контент, нарушающий правила; • предложить пользователям простой и доступный способ предупреждения изготовителя контента о нарушении каких-либо правил в онлайновом сообществе; • удалять контент, нарушающий правила; Перед выгрузкой специально подобранного с учетом возраста контента на сайт социальной сети необходимо ознакомиться с положениями и условиями работы сайта. Внимательно относиться к требованиям по минимальному возрасту доступа на разных сайтах социальных сетей. Положения и условия работы каждого онлайнового пространства, кроме прочего, должны включать четкие механизмы сообщения о нарушении подобных правил.
Создание более безопасной, соответствующей возрасту онлайновой среды	Компании, предлагающие специально подобранный контент, могут оказать помощь в создании более безопасной, более увлекательной цифровой среды для детей и молодых людей всех возрастов, предпринимая следующие действия:
	Работать с другими представителями отрасли в плане разработки классификации контента/систем возрастной оценки на основе приемлемых национальных и международных стандартов и в соответствии с подходами, применяемыми в равнозначных средствах информации. По мере возможности классификация контента должна быть согласованной в рамках разных медийных платформ, например, рекламный ролик о фильме в кинотеатре и на смартфоне следует относить к одному и тому же классу.
	Разработать дружественные ребенку и соответствующие возрасту продукты для детей и молодых людей на основе проектируемой безопасности, дополняемые надежными системами проверки возраста.
	Помочь родителям и прочим лицам в принятии решений о соответствии контента возрасту детей и молодых людей, создать приложения и услуги во всех средствах информации для согласования с системами оценки контента. Принять соответствующие методы подтверждения возраста, чтобы предотвратить доступ детей и молодых людей к контенту, сайтам или интерактивным услугам, неприемлемым для определенного возраста. Предусмотреть рекомендации и напоминания о характере и возрастной классификации используемого контента.
	Компания, предлагающая аудиовизуальные и мультимедийные услуги, может установить собственную систему персональных идентификационных номеров для пользователей, желающих получать доступ к контенту, потенциально вредоносному для детей.

Создание более безопасной, соответствующей возрасту онлайновой среды (*продолжение*)	Обеспечить прозрачность в отношении ценообразования для продуктов и услуг, а также сбора информации о пользователях. Обеспечить соответствие политики сбора данных с действующими законами, затрагивающими личную жизнь детей и молодых людей, включая рассмотрение необходимости получения согласия родителей на сбор коммерческими предприятиями информации от ребенка или о нем.
	Обеспечить четкое распознавание сообщений рекламного и коммерческого характера. Контролировать размещенный в интернете контент и адаптировать его под различные группы пользователей, которые, вероятнее всего, будут просматривать его, установив, например, приемлемые правила онлайновой рекламы для детей и молодых людей. Если предлагаемый контент включает интерактивные элементы, например, комментирование, онлайновые форумы, социальные сети, игровые платформы, чаты или доски сообщений, включить в условия обслуживания и инструкции для пользователей четкий набор "внутренних правил", составленных на понятном клиентам языке.
	Перед запуском онлайновой услуги принять решение о желаемом уровне участия. Услуги, направленные на детей, должны представлять только тот контент, который приемлем для юной аудитории. В случае сомнений можно обратиться за консультацией в национальные органы по вопросам защиты детей.
	Предоставить четкую и опирающуюся на факты маркировку контента. Следует помнить, что пользователи могут столкнуться с неприемлемым контентом, переходя по ссылкам на сайты третьих сторон в обход контекстных страниц.
Обучение детей, родителей и педагогов правилам детской безопасности и ответственного использования ими ИКТ	Компании, предлагающие специально подобранный цифровой контент, могут дополнить технические меры обучающими мероприятиями, расширяющими возможности детей, предпринимая следующие действия:
	Предоставить клиентам конкретную и четкую информацию о контенте, в частности указать его тип, возрастные оценки/ограничения, правила в отношении грубости и насилия наряду с доступными инструментами родительского контроля, а также о способах сообщения о неправомерном использовании и неприемлемом или незаконном контенте и порядке рассмотрения таких сообщений. В интерактивном мире такую информацию следует предоставлять в форме маркировки контента по каждой программе.
	Поощрять участие взрослых, особенно родителей, опекунов и педагогов, в потреблении онлайнового контента детьми и молодыми людьми, чтобы помогать и направлять их в выборе контента при его покупке, а также способствовать формированию определенных правил поведения. Помочь детям (а также родителям и опекунам) научиться управлять временем, которое они проводят у экрана монитора, и понять, как пользоваться технологиями, не в ущерб своему благополучию, в том числе знать, когда следует остановиться и переключиться на что-то другое.
	Разработать правила пользования, составленные на понятном и доступном языке, чтобы стимулировать детей и молодых людей быть более бдительными и ответственными при навигации по интернету.
	Создать соответствующие возрасту инструменты, например, обучающие программы и центры помощи. По мере возможности сотрудничать с онлайновыми или персональными профилактическими программами и консультационными клиниками. Например, при наличии риска чрезмерного вовлечения детей и молодых людей в определенные технологии, например, игры, возникновения у них сложностей в формировании личных взаимоотношений или участии в полезных для здоровья физических видах деятельности, на сайте можно разместить ссылку службы помощи или консультационного центра. Всю информацию о безопасности, включая ссылки на рекомендации, сделать заметной, легкодоступной и понятной в том случае, если достаточно большая доля онлайнового контента адресована детям и молодым людям.

Обучение детей, родителей и педагогов правилам детской безопасности и ответственного использования ими ИКТ (*продолжение*)	Предложить инструменты родительского управления, например, функцию "блокирования" для контроля контента, доступ к которому возможен через определенный браузер.
	Сотрудничать с родителями, чтобы гарантировать, что раскрываемая в интернете информация о детях не представляет для них никакого риска. Способы идентификации детей в рамках специально подобранного контента должны быть продуманы и обусловлены контекстом. По мере возможности получать информированное согласие детей при их появлении в программах, фильмах, видеоматериалах и пр. и уважать их право на отказ от участия.
Содействие продвижению цифровых технологий как средства усиления участия в жизни гражданского общества	Компании, предлагающие специально подобранный цифровой контент, могут поощрять детей и молодых людей и предоставлять им соответствующие возможности, поддерживая их право на участие, предпринимая следующие действия:
	Разработать и/или предложить выбор заставляющего думать, образовательного, увлекательного и интересного контента высокого качества согласно возрасту, который помогает детям и молодым людям и наполняет окружающих их мир смыслом. Помимо своей привлекательности и полезности, надежности и безопасности, такой контент может способствовать физическому, умственному и социальному развитию детей и молодых людей, предоставляя новые возможности для развлечений и обучения. В особенности приветствуется контент, который дает детям возможность понять разнообразие окружающего мира, выстраивая позитивные ролевые модели.

5.3 Функция C: размещение создаваемого пользователями контента и установление связей между пользователями

Было время, когда в онлайновой среде доминировали взрослые, но теперь уже ясно, что основными участниками становятся дети и молодые люди, которые, пользуясь множеством платформ, создают и обмениваются просто гигантскими объемами пользовательского контента. Данная группа, среди прочего, охватывает услуги социальных сетей, приложений и веб-сайтов, связанных с творческой реализацией.

Услуги, соединяющие пользователей друг с другом можно разделить на три категории:

- приложения, преимущественно, используемые для обмена сообщениями (Facebook Messenger, Groupme, Line, Tinder, Telegram, Viber, WhatsApp);
- услуги, преимущественно, социальных сетей, основанных на генерируемом пользователями контенте и позволяющих им обмениваться контентом и быть на связи как внутри, так и за пределами своих сетей (Instagram, Facebook, SnapChat, TikTok);
- приложения, преимущественно, используемые для прямого потокового вещания (Periscope, BiGo Live, Facebook Live, Houseparty, YouTube Live, Twitch, GoLive).

Поставщики услуг запрашивают минимальный возраст для регистрации на своих платформах, однако контролировать его соблюдение сложно, поскольку проверка возраста полагается на сообщаемые сведения. Большинство услуг, соединяющих новых пользователей друг с другом, также допускают функции обмена местоположением, что делает детей и молодых людей, пользующихся такими услугами, более восприимчивыми к опасностям реального мира.

В Таблице 4, основу которой составляют правила, принятые одной из наиболее крупных социальных сетей, представлены руководящие указания для поставщиков услуг, связанных с размещением создаваемого пользователями контента и соединением новых пользователей, в отношении политики и действий, которые они могут предпринять с целью усиления защиты и участия ребенка в онлайновой среде.

Таблица 4 – Контрольный перечень по COP для функции C: размещение создаваемого пользователями контента и установление связей между пользователями

Включение положений о правах ребенка во все соответствующие корпоративные политики и процессы управления	Поставщики услуг размещения создаваемого пользователями контента и соединения пользователей могут выявлять, предотвращать и ослаблять неблагоприятное влияние ИКТ на права детей и молодых людей, а также определять возможности для содействия реализации прав детей и молодых людей.
	См. общие руководящие указания в Таблице 1.
Разработка стандартных методов обращения со CSAM	Совместно с государственными и правоохранительными органами, представителями гражданского общества и горячих линий компании, предоставляющие услуги размещения создаваемого пользователями контента и соединения пользователей, могут играть важную роль в борьбе со CSAM, предпринимая следующие действия:
	Установить для всех сайтов процедуры оказания незамедлительной помощи правоохранительным органам в чрезвычайных ситуациях и при исполнении обычных запросов.
	Закрепить всестороннее сотрудничество с правоохранительными органами при расследовании случаев обнаружения или сообщения о незаконном контенте и определить детали соответствующих мер ответственности, например штрафов или отмены льготной оплаты услуг.
	Работать с внутренними службами, в частности с отделом по работе с клиентами, отделом по профилактике мошенничества и службой охраны с целью обеспечения возможности сообщать о предполагаемых случаях незаконного контента непосредственно правоохранительным органам и на горячие линии. В идеале, такая процедура не должна подвергать исполнительный персонал воздействию вредоносного контента или способствовать повторному насилию над пострадавшим ребенком/пострадавшими детьми и молодыми людьми. В тех ситуациях, когда сотрудники могут подвергаться воздействию оскорбительного материала, установить правила или внедрить программу поддержки для восстановления их морального здоровья, безопасности и благополучия.
	Включить в положения и условия обслуживания пункты, запрещающие незаконный контент и поведение, особо подчеркивая следующие моменты: • вредоносный контент, включая предполагаемые случаи груминга детей с намерением применения насилия с установлением контакта или без контакта, не допускается; • незаконный контент, включая выгрузку и дальнейшее распространение CSAM, не допускается; • компания будет обращаться и всесторонне сотрудничать с правоохранительными органами при расследовании случаев сообщения или обнаружения незаконного контента или нарушения политики защиты детей.
	Документально оформить политики компании по обращению со CSAM, начиная с мониторинга и заканчивая окончательным переносом и уничтожением контента. Включить в состав документов перечень сотрудников, ответственных за выполнение различных операций с материалами.
	Принять правила, регулирующие вопросы прав собственности на создаваемый пользователями контент, включая возможность удаления такого контента по просьбе пользователя. Удалять контент, нарушающий правила поставщика услуг, и предупреждать опубликовавших его пользователей о нарушении.
	Указать, что к пользователям, не сумевшим выполнить требования правил приемлемого использования, будут применяться определенные меры, в частности: • удаление контента, приостановление обслуживания учетных записей или их закрытие; • блокирование возможности обмениваться определенными типами контента или использовать определенные функции;

Разработка стандартных методов обращения со CSAM (*продолжение*)	• предотвращение их возможности контактировать с детьми; • сообщение в правоохранительные органы.
Разработка стандартных методов обращения с материалами, связанными с сексуальными злоупотреблениями в отношении детей	Содействовать применению механизмов обратной связи по CSAM или по любому другому незаконному контенту и убедиться, что клиенты знают, как сообщить о факте обнаружения таких материалов. Создать системы и выделить специально обученных сотрудников для оценки конкретных случаев и принятия соответствующих мер. Организовать полноценные и обеспеченные необходимыми ресурсами оперативные группы поддержки пользователей. В идеале, такие группы должны пройти обучение по правилам разрешения инцидентов различных типов, чтобы гарантировать достаточное реагирование и принятие приемлемых мер. Поданная пользователем жалоба передается соответствующему сотруднику в зависимости от типа инцидента. Кроме того, компания может организовать специальные группы по рассмотрению ходатайств пользователей в тех случаях, когда сообщения отсылаются по ошибке.
	Утвердить порядок немедленного удаления или блокирования доступа к CSAM, включая процедуры уведомления и отключения, направленные на удаление незаконного контента сразу же после его выявления. Убедиться, что третьи лица, с которыми компания установила договорные отношения, применяют аналогичные надежные процедуры уведомления и отключения. Если это разрешено законодательством, материал может сохраняться в качестве доказательства совершенного преступления при его расследовании.
	Разработать технические системы обнаружения заведомо незаконного контента и предотвращения его выгрузки в сеть, в том числе в приватных группах, или маркировки такого контента для немедленного анализа службой безопасности компании. Принять все соответствующие меры для защиты услуг от неправомерного использования с целью размещения, распространения или создания CSAM. По мере возможности разработать упреждающие технические средства для анализа связанных с профилем объектов и метаданных с целью выявления преследуемого по закону поведения или схем и принятия соответствующих мер.
	Если приложение или услуга позволяют клиентам загружать или хранить фотографии на серверах, принадлежащих компании или обслуживаемых ею, установить процессы и инструменты для распознавания изображений, которые потенциально могут содержать CSAM. Предусмотреть упреждающие средства идентификации, например технологии сканирования или проверки человека.
Создание более безопасной, соответствующей возрасту онлайновой среды	Поставщики услуг размещения создаваемого пользователями контента и соединения пользователей могут оказать помощь в создании более безопасной, более увлекательной цифровой среды для детей разных возрастов, предпринимая следующие действия:
	Включить в условия обслуживания и инструкции для пользователей составленные на понятном клиентам языке "внутренние правила", определяющие следующие моменты: • характер услуги и ожидания в отношении ее пользователей; • что является и не является приемлемым с точки зрения контента, поведения и языка, а также запрет незаконного использования; • последствия соответственно степени допущенного нарушения, например сообщение в правоохранительные органы или приостановление обслуживания учетной записи пользователя.

Создание более безопасной, соответствующей возрасту онлайновой среды (*продолжение*)	Важнейшие вопросы безопасности и законности должны быть представлены в соответствующем возрасту формате (т. е. с использованием интуитивных значков и символов), как при входе в систему, так и своевременно при выполнении различных действий на сайте.
	Упростить для клиентов процесс сообщения о своих сомнениях в связи с неправомерным использованием контента сотрудникам отдела по работе с клиентами, установив стандартный и доступный порядок рассмотрения разного рода проблем, таких как получение нежелательных материалов (спам, травля) или просмотр неприемлемого контента.
	Установить соответствующие возрасту настройки обмена контентом и видимости. Например, ввести более строгие ограничения в настройках конфиденциальности и видимости для детей и молодых людей по сравнению с настройками по умолчанию для взрослых.
	Ввести минимальные возрастные требования и способствовать проведению исследований и разработок в области новых систем проверки возраста (например, биометрии), используя при разработке таких инструментов известные международные стандарты. Принять меры по выявлению и удалению учетных записей малолетних пользователей, которые неверно указали свой возраст с целью получения доступа. При этом следует учитывать неизбежность сбора дополнительных данных для выполнения этого требования и необходимость ограничения сбора, хранения и обработки такой информации. Если такие меры еще не применяются, установить приемлемые процессы регистрации, позволяющие определить, достаточно ли зрелыми являются пользователи, чтобы получать доступ к контенту или услуге, при этом такие процессы не должны ставить под угрозу идентичность, местоположение и персональные данные. Использовать утвержденные на национальном уровне функциональные системы проверки возраста по мере применимости, при условии наличия достаточных мер по обеспечению конфиденциальности данных детей. Обеспечить наличие функции обратной связи или справочной службы/центра, поощряя пользователей сообщать о лицах, фальсифицирующих сведения об их возрасте.
	Защитить юных пользователей от получения нежелательных сообщений и гарантировать соблюдение установленных правил конфиденциальности и сбора информации.
	Найти способы проверки размещаемых на сайтах изображений и видеоматериалов и удалять неприемлемый контент в случае его обнаружения. Полезными в этом плане могут оказаться такие инструменты, как сканирование хэш-индексов известных изображений и программы распознавания изображений. В отношении услуг, связанных с детьми, фотографии и видеоматериалы могут проходить предварительную проверку, чтобы не допустить публикацию детьми уязвимой персональной информации о них самих и других лицах.
	Существует целый ряд средств контроля доступа к создаваемому пользователями контенту и защиты детей и молодых людей от неприемлемого или незаконного контента в онлайновой среде. В этой связи важно установить проверку надежности паролей как шаг вперед на пути защиты детей и молодых людей в среде игровых и прочих социальных сетей. В числе других средств можно назвать: • проверку дискуссионных групп с целью выявления опасных тем для обсуждения, агрессивных высказываний и противоправного поведения, а также удаление подобного контента в случае обнаружения нарушения правил пользования; • разработку инструментов активного поиска и удаления контента, являющегося незаконным или нарушающим положения и условия обслуживания компании, а также инструментов, предотвращающих выгрузку заведомо незаконного контента на сайт;

Создание более безопасной, соответствующей возрасту онлайновой среды (*продолжение*)	• предварительное модерирование на досках сообщений силами специальной команды модераторов контента для детей и молодых людей, которая следит за контентом, противоречащим опубликованным "внутренним правилам". Каждое сообщение может проверяться до его публикации, при этом модераторы выявляют и отмечают подозрительных пользователей, а также пользователей, попавших в беду; • организацию группы ведущих членов сообщества, которая служит исходной точкой контакта для модераторов в тех случаях, когда у них возникают сомнения в отношении какого-либо пользователя.
	Ответственно относиться к проверке контента коммерческого характера, включая форумы, социальные сети и игровые сайты. Внедрить приемлемые стандарты и правила защиты детей от не соответствующей возрасту рекламы и установить четкие ограничения по онлайновой рекламе для детей и молодых людей.
Обучение детей, родителей и педагогов правилам детской безопасности и ответственного использования ими ИКТ	Поставщики услуг размещения создаваемого пользователями контента и соединения пользователей могут предпринимать следующие действия, направленные на повышение уровня образования и расширение прав и возможностей, в дополнение к техническим мерам:
	Создать раздел, в котором будут публиковаться связанные с безопасностью советы, статьи, заметки и обсуждения на темы цифрового гражданства, а также ссылки на полезный контент сторонних экспертов. Советы по безопасности должны быть заметными и составленными на доступном для понимания языке. Поставщикам платформ также рекомендуется установить однотипные принципы навигации на разных устройствах, включая компьютеры, планшеты или мобильные телефоны.
	Предложить родителям четкую информацию о доступных типах контента и услуг, в частности предоставить разъяснения о сайтах социальных сетей и услугах, предоставляемых с учетом местоположения пользователя, о том, как осуществляется доступ в интернет с мобильных устройств, а также о возможных вариантах применения родительского контроля.
	Информировать родителей о том, как можно сообщить о злоупотреблениях, неправомерном использовании и неприемлемом или незаконном контенте, и как такие сообщения будут рассматриваться. Предоставить им сведения о том, какие услуги ограничиваются по возрасту, а также о других способах безопасного и ответственного поведения при пользовании интерактивными услугами.
	Установить основанную на принципе "доверия и репутации" систему, поощряющую хорошее поведение, что позволит сверстникам передавать друг другу опыт на собственном примере. Содействовать развитию понимания важности социальной обратной связи, способствуя тому, чтобы люди шли навстречу другим пользователям или друзьям, которым они доверяют, помогая решить конфликт или начать разговор о вызывающем беспокойство контенте.
	Предусмотреть рекомендации и напоминания о характере предоставляемой услуги или контента, а также о том, как безопасно им пользоваться. Включить в структуру интерактивных услуг инструкции для сообщества, например в форме всплывающих подсказок по безопасности, напоминающих пользователям о приемлемом и безопасном поведении, в частности о том, что не следует раскрывать свои контактные данные.
	Сотрудничать с родителями и предоставлять им инструкции, чтобы гарантировать, что раскрываемая в интернете информация о детях не представляет для них никакого риска. По мере возможности получать информированное согласие детей при их появлении в созданном ими самими контенте и уважать их право на отказ.
Содействие продвижению цифровых технологий как средства усиления участия в жизни гражданского общества	Поставщики услуг размещения создаваемого пользователями контента и соединения пользователей могут поощрять детей и молодых людей и предоставлять им соответствующие возможности, поддерживая их право на участие.
	См. общие руководящие указания в Таблице 1.

5.4 Функция D: системы на основе искусственного интеллекта

На фоне повышенного внимания к технологиям глубокого обучения термины "искусственный интеллект", "машинное обучение" и "глубокое обучение" среди широкой общественности являются в определенном смысле взаимозаменяемыми, отображая концепцию копирования "разумного" поведения машинами. В этом разделе мы сосредоточимся на том, как машинное обучение и глубокое обучение влияют на жизни детей и, в конечном итоге, на их права.

"Ввиду экспоненциального продвижения технологий на базе искусственного интеллекта за последние несколько лет нынешние международные схемы защиты прав детей не охватывают однозначно многие вопросы, вставшие в результате развития и использования искусственного интеллекта. Тем не менее, очевидно выделяются некоторые права, которые могут оказаться под воздействием таких технологий, что служит отправной точкой для анализа того, каким образом, положительно или отрицательно, эти новые технологии могут влиять на права детей, в частности на право на личную жизнь, образование, игру и отсутствие дискриминации"[18].

Применение ИИ может повлиять на воздействие, оказываемое на детей различными услугами, используемыми в социальных сетях, например на платформах потокового вещания. Алгоритмы машинного обучения, службы рекомендаций, применяемые, прежде всего, на популярных платформах обмена видеоматериалами, оптимизируются для максимального повышения количества просмотров определенных роликов в течение заданного времени[19]. Технологии сенсорных экранов и проектирование таких платформ позволяют детям даже самого младшего возраста перемещаться по такому контенту. Особое беспокойство вызывает то, что алгоритмы, использующие рекомендуемые видеоматериалы, могут завести детей в ловушку "пузыря фильтров" с некачественным или неприемлемым контентом. Поскольку дети особенно восприимчивы к рекомендациям контента, шокирующие "связанные видео" могут привлечь их внимание и отвести в сторону от более дружественных ребенку алгоритмов[20].

ИИ также влияет на защиту ребенка в онлайновой среде в связи с умными игрушками. Четкие процессы, используемые в работе умных игрушек сопряжены со своими сложностями, т. е. игрушка (которая контактирует с ребенком), мобильное приложение, которое действует как точка доступа для соединения Wi-Fi, и персонализированная учетная запись игрушки/потребителя, в которой хранятся данные. Такие игрушки обмениваются информацией с облачными серверами, где хранятся и обрабатываются данные, предоставленные детьми, взаимодействующими с игрушками. Такая модель вызывает опасения в связи с конфиденциальностью в случае недостаточной безопасности на каком-либо из уровней, что подтверждается многочисленными случаями взлома, приводившими к утечке персональных данных. Более того, некоторые взломанные устройства (включая умные устройства, соединенные с интернетом, такие как радио-няни, голосовые помощники и пр.) могут использоваться для отслеживания пользователей без их ведома или согласия.

При внедрении механизмов реагирования на выявленные угрозы для детей, пользующихся такими устройствами, с помощью, например, предоставления советов и рекомендаций на основе установленного поведения (как упоминалось ранее при описании приложения BBC Own It), крайне важно, чтобы компании, разрабатывающие умные устройства, составляли подобные рекомендации, опираясь на объективные данные, и разрабатывали их на основе консультаций со специалистами по защите детей и охране их интересов.

---

18 UNICEF and UC Berkeley "Executive Summary: Artificial Intelligence and Children's Rights", 2018.
19 Ibid.
20 Ibid

При том, что некоторые компании пропагандируют принципы этического использования ИИ[21], не вполне ясно, существуют ли какие-либо общественные правила в области ИИ и детей[22]. Ряд технологических и отраслевых ассоциаций и научных групп по информатике составили проект перечня этических принципов в отношении ИИ[23]. Однако, эти принципы не имеют четкой связи с правами ребенка, способами, в рамках которых технологии ИИ могут представлять риск для детей, или упреждающими планами по смягчению таких рисков.

"Как и корпорации, правительства по всему миру принимают стратегии, позволяющие лидировать в области разработки и использования ИИ, формирования среды благоприятной для новаторов и корпораций"[24]. Тем не менее, не вполне понятно, как такие национальные стратегии соотносятся с правами ребенка.

Улучшение работы Facebook с контентом, связанным с самоубийством и нанесением себе увечий

В 2019 году компания Facebook начала серию регулярных консультаций со специалистами из разных стран мира по ряду наиболее сложных тем, связанных с самоубийством и членовредительством. В числе прочего рассматривались вопросы реагирования на записки о самоубийстве, рисков, связанных с депрессивным контентом в интернете и освещением суицида в новостях. Дополнительные подробности этих встреч приводятся на новой странице "Предотвращение самоубийств" Facebook в разделе "Центр безопасности". Эти консультации позволили сделать несколько улучшений в способах обращения Facebook с таким типом контента. В частности, политика в отношении нанесения себе увечий была усилена запретом на изображения с ранениями во избежание ненамеренного содействия членовредительству или его инициирования. Даже если кто-то обращается за помощью или демонстрирует себя в поисках помощи для лечения, Facebook теперь маскирует зажившие раны на изображениях. Контент подобного рода теперь выявляется с помощью ИИ, при этом действия в связи с потенциально вредоносным контентом, включая его удаление или добавление масок, могут предприниматься автоматически. С апреля по июнь 2019 года Facebook приняла меры в отношении более 1,5 миллионов единиц контента о суициде и членовредительстве на своем сайте, причем более 95 процентов из них были выявлены до сообщения о них пользователями. За тот же период времени Instagram рассмотрела более 800 тысяч единиц аналогичного контента, из которых более 77 процентов были обнаружены до получения сообщений о них от пользователей.

Выявление потенциальной травли или насилия между сверстниками в реальном времени и информирование пользователей

Instagram внедряет ИИ для искоренения такого поведения как оскорбления, публичное высмеивание и неуважение. Используя высокотехнологичные инструменты обратной связи, модераторы могут быстро закрывать учетные записи, которые принадлежат лицам, осуществляющим травлю в интернете.

[21] См. Microsoft, "Salient Human Rights Issues", Report- FY17; и Google, "Responsible Development of AI" (2018).
[22] Официальный блог Microsoft "The Future Computed: Artificial Intelligence and its role in society", 2018 г.
[23] The Guardian, "'Partnership on AI' formed by Google, Facebook, Amazon, IBM and Microsoft", 2016.
[24] Ibid

Передовой опыт: использование искусственного интеллекта для выявления материалов, связанных с сексуальными злоупотреблениями в отношении детей

Опираясь на щедрый вклад Microsoft в борьбу с детской эксплуатацией в форме PhotoDNA и недавний запуск Google Content Safety API, Facebook разработала технологии для обнаружения контента, связанного с сексуальными злоупотреблениями в отношении детей.

Эти технологии, получившие название PDQ и TMK+PDQF, являются частью набора инструментов, которые Facebook использует для обнаружения вредоносного контента. В число других алгоритмов и инструментов, имеющихся в арсенале отрасли, входят pHash, aHash и dHash. Применяемый Facebook алгоритм сопоставления фотографий PDQ во многом перекликается с pHash, однако он был разработан обособленно и с нуля на базе независимого программного обеспечения. Технология сопоставления видеоматериалов TMK+PDQF была разработана совместно группой исследования ИИ Facebook и учеными-специалистами из Университета Модены и Реджо-Эмилия в Италии.

Эта технология обеспечивает эффективный способ хранения файлов в виде коротких цифровых хэшей, позволяющих определить, являются ли два файла одинаковыми или похожими даже без наличия оригинального изображения или видеоролика. Такими хэшами, кроме прочего, можно легко обмениваться с другими компаниями и неприбыльным организациями.

PDQ и TMK+PDQF были разработаны для широкомасштабного применения с поддержкой хэширования видеокадров и приложений в реальном времени.

Некоторые рекомендации для компаний по согласованию их принципов при проектировании и внедрении решений на базе ИИ, направленных на детей, представлены в Таблице 5.

Рекомендации основаны на работе ЮНИСЕФ по разработке глобальных руководящих указаний по ИИ и детям, которые будут предназначены для государственных органов и отраслевых предприятий. Более подробную информацию о проекте можно найти по адресу https://www.unicef.org/globalinsight/featured-projects/ai-children. В данных рекомендациях также учтены положения отчета ЮНИСЕФ и UC Berkeley по ИИ и правам ребенка.[25]

Таблица 5 – Контрольный перечень по COP для функции D: системы на основе ИИ

Включение положений о правах ребенка во все соответствующие корпоративные политики и процессы управления	Поставщики услуг на основе систем, управляемых ИИ, могут выявлять, предотвращать и ослаблять неблагоприятное влияние ИКТ на права детей и молодых людей, а также определять возможности для содействия реализации прав детей и молодых людей.
	Системы ИИ необходимо проектировать, разрабатывать, внедрять и исследовать, уважая, содействуя и соблюдая права детей, закрепленные в Конвенции о правах ребенка. Детство, которое все больше протекает в цифровой среде, – это время, требующее особой заботы и помощи. Системы ИИ следует использовать таким образом, чтобы реализовать полный потенциал такой поддержки.
	Следует применять всеохватный подход к проектированию при разработке продуктов, предназначенных для детей, чтобы максимально расширить гендерное, географическое и культурное разнообразие, вовлекая большой спектр заинтересованных сторон, в том числе родителей, учителей, детских психологов и, по мере возможности, самих детей.
	Необходимо установить рамочную основу управления, включая этические нормы, законы, стандарты и регуляторные органы, предусматривающую процессы, которые обеспечивают применение систем ИИ без нарушения прав ребенка.

[25] UNICEF and UC Berkeley, "Executive Summary: Artificial Intelligence and Children's Rights", 2018.

Разработка стандартных методов обращения со CSAM	Совместно с государственными и правоохранительными органами, представителями гражданского общества и горячих линий поставщики услуг на основе систем, управляемых ИИ, могут играть важную роль в борьбе со CSAM, предпринимая следующие действия:
	См. общие руководящие указания в Таблице 1.
Создание более безопасной, соответствующей возрасту онлайновой среды	Поставщики услуг на основе систем, управляемых ИИ, могут оказать помощь в создании более безопасной, более увлекательной цифровой среды для детей разных возрастов, предпринимая следующие действия:
	Принять междисциплинарный подход при разработке технологий, воздействующих на детей, и консультироваться с гражданским обществом, включая образовательные учреждения, чтобы определить возможные воздействия таких технологий на права различных групп потенциальных конечных пользователей.
	Применять принципы проектируемой безопасности и проектируемой конфиденциальности для продуктов и услуг, предназначенных или часто используемых детьми.
	Поскольку системы ИИ требуют больших объемов данных, компании, применяющие ИИ в своих услугах, должны проявлять особую бдительность в отношении сбора, обработки, хранения, продажи и публикации персональных данных детей. Системы ИИ должны быть прозрачными, то есть необходимо обеспечить возможность установить, как и почему система приняла определенное решение или, в случае с роботом, почему он выполнил именно это действие. Такая прозрачность крайне важна для формирования доверия и обеспечения проверки, расследования и обращения за помощью в предполагаемых случаях причинения вреда детям. Обеспечить наличие функциональных и правовых механизмов для обращения за помощью, если детям был нанесен ущерб в связи с системой ИИ или при поступлении такой претензии. Необходимо установить процессы для своевременного исправления всех дискриминирующих последствий и учредить надзорные органы для подачи обращений и непрерывного мониторинга безопасности и защиты детей. Подотчетность и механизмы исправления являются тесно связанными друг с другом.
	Разработать планы по обращению с особо чувствительными данными, включая порядок раскрытия злоупотреблений или других вредоносных материалов, которые могут использоваться во внутренней среде компании, через ее продукцию. Сбор данных о детях на цифровых платформах и в системах ИИ должен быть минимальным с предоставлением детям максимальной возможности контролировать данные, которые они создают. Условия использования должны быть понятными детям, способствуя повышению их осведомленности и свободе выбора.
Обучение детей, родителей и педагогов правилам детской безопасности и ответственного использования ими ИКТ	Поставщики услуг на основе систем, управляемых ИИ, в дополнение к техническим мерам, могут содействовать повышению уровня образования и расширению прав и возможностей.
	Необходимо обеспечить возможность разъяснения цели систем ИИ пользователям-детям и их родителям или опекунам, чтобы расширить их возможности при принятии решения об использовании данной платформы или отказе от него.
Содействие продвижению цифровых технологий как средства усиления участия в жизни гражданского общества	Поставщики услуг на основе систем, управляемых ИИ, могут поощрять детей и молодых людей и предоставлять им соответствующие возможности, поддерживая их право на участие, предпринимая следующие действия:
	См. общие руководящие указания в Таблице 1.

Использование технологических достижений для защиты и обучения детей	Системы, управляемые ИИ, необходимо разрабатывать с учетом поддержки развития и благополучия детей во всех элементах проектирования, разработки и внедрения. Отправной точкой должны служить лучшие из имеющихся и широко признанные показатели развития и благополучия. Компаниям следует вкладывать средства в исследования и разработку этических инструментов на базе ИИ с целью выявления фактов CSAE в интернете, а также домогательств и травли в онлайновой среде в сотрудничестве с ведущими специалистами по правам ребенка и самими детьми. Необходимо применять достижения в технологиях ИИ с целью предоставления детям соответствующей возрасту информации без ущемления их идентичности, без раскрытия их местоположения и персональных данных.

Справочные материалы

Текст GDPR (Регламент (ЕС) 2016/679 Европейского Парламента и Совета Европейского Союза от 27 апреля 2016 года о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий регламент о защите персональных данных)) и текст, опубликованный в Официальном бюллетене ЕС.

Пересмотренная Директива AVMS (об аудиовизуальных медиа-услугах), вносящая поправки в Директиву 2010/13/EU о координировании некоторых положений закона, норм и административных актов в Государствах-Членах в отношении положений об аудиовизуальных медиа-услугах (Директива об аудиовизуальных медиа-услугах) ввиду изменений, происходящих на рынке, а также текст, опубликованный в Официальном бюллетене ЕС.

Политика BBC:

- Политика по защите и охране ребенка, редакция 2017 года, пересмотрена в 2018 году, и обновленная редакция 2019 года
- Работа с молодыми людьми и детьми в BBC;
- Общие принципы для независимых продюсерских компаний, работающих в проектах BBC, по разработке правил внешних поставщиков в отношении защиты детей;
- Руководящие принципы: Взаимодействие с детьми и молодыми людьми в онлайновой среде в отношении редакторских руководящих указаний по деятельности в онлайновой среде.

Расследование, подтверждающее несоблюдение правил проверки возраста в социальных сетях в Соединенном Королевстве: 2016 г., 2017 г.; 2020 г.

Глоссарий

Следующие ниже определения приводятся, главным образом, на основании действующей терминологии, закрепленной Конвенцией о правах ребенка 1989 года, а также выработанной Межведомственной рабочей группой по сексуальной эксплуатации детей в Руководящих указаниях по терминологии в области защиты детей от сексуальной эксплуатации и сексуальных злоупотреблений, 2016 год (Люксембургские руководящие указания), Советом Европы в Конвенции о защите детей от сексуальной эксплуатации и сексуальных злоупотреблений, 2007 год, и ЮНИСЕФ в докладе Global Kids Online, 2019 год.

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[26].

Искусственный интеллект

В самом широком смысле термин "искусственный интеллект (ИИ)" 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 (эти системы описываются как "слабый" или "средний" ИИ, например системы распознавания лиц или голоса и системы управления автомобилем)[27].

Системы искусственного интеллекта

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. Системы ИИ предназначены для функционирования с различными уровнями автономности[28].

Alexa

Amazon Alexa, известная как просто Alexa, представляет собой систему ИИ – виртуального помощника, разработанную Amazon. Она поддерживает такие функции как голосовое взаимодействие, проигрывание музыки, составление списка дел, установка будильника, проигрывание подкастов и аудиокниг, сообщение прогноза погоды, данных о ситуации на дорогах, спортивных событиях и другой информации в реальном времени, например новостей. Alexa также может контролировать несколько "умных" устройств, функционируя как система бытовой автоматизации. Пользователи могут расширять функционал Alexa путем установки "умений" (дополнительных функциональных возможностей, разрабатываемых сторонними поставщиками, которые в других случаях обычно именуются приложениями, например программ отслеживания погоды и аудиофункций)[29].

Наилучшие интересы ребенка

Понятие, описывающее все элементы, необходимые для принятия решения в конкретной ситуации в отношении конкретного ребенка или группы детей[30].

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[31].

Сексуальная эксплуатация и сексуальные злоупотребления в отношении детей

Данное понятие описывает все формы сексуальной эксплуатации и сексуальных злоупотреблений, 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"[32], а также "половой контакт, как правило с применением силы в отношении лица без его согласия"[33]. Сексуальная эксплуатация и сексуальные злоупотребления в отношении детей (CSEA) все чаще происходят с использованием интернета или тем или иным образом связаны с онлайновой средой.

---

26 ЮНИСЕФ и МСЭ "Руководящие указания для отрасли по защите ребенка в онлайновой среде", 2014 г.
27 Council of Europe, "What's AI?".
28 OECD, "Recommendation of the Council on Artificial Intelligence", 2019.
29 ЮНИСЕФ и МСЭ "Руководящие указания для отрасли по защите ребенка в онлайновой среде", 2014 г.
30 См. текст Конвенции Организации Объединенных Наций о правах ребенка.
31 ЮНИСЕФ и МСЭ "Руководящие указания для отрасли по защите ребенка в онлайновой среде", 2014 г.
32 Статья 34 Конвенции Организация Объединенных Наций о правах ребенка.
33 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Luxembourg Guidelines), 2016.

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

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[34]. 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" (CSAM). Этот термин согласуется с Руководящими указаниями Комиссии по широкополосной связи и Моделью реагирования на национальном уровне, разработанной Глобальным альянсом WePROTECT[35], и более точно описывает соответствующий контент. Порнографией считается правомерная коммерческая отрасль, и, как отмечается в Люксембургских руководящих указаниях, использование такого термина: "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". Пользуясь термином CSAM, мы имеем в виду материалы, представляющие собой деяния, 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.

Определение таких понятий, как "материалы, связанные с сексуальными злоупотреблениями в отношении детей, созданные компьютером или цифровыми средствами", см. в Люксембургских руководящих указаниях.

Дети и молодые люди

Понятие, описывающее всех лиц моложе 18 лет, при этом "детьми" (или "детьми младшего возраста" в настоящих Руководящих указаниях МСЭ) считаются все лица моложе 15 лет, а "молодыми людьми" – все лица возрастной группы 15–18 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[36].

Кибертравля

Кибертравля означает намеренно агрессивное действие, неоднократно осуществляемое группой лиц или отдельным лицом при помощи цифровых технологий и направленное против жертвы, которой трудно защитить себя[37]. 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 или текстовых сообщениях), распространение сплетен и ложной информации о жертве или намеренное исключение ее из онлайнового общения"[38].

---

34 The Luxembourg Guidelines (as above), 2016 and the UNICEF Global Kids Online report, 2019.

35 Broadband Commission for Sustainable Development, "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online", 2019; WePROTECT Global Alliance, "Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response", 2016.

36 Jeremy Greenberg, "Dangerous Games: Connected Toys, COPPA, and Bad Security", Georgetown Law Technology Review, 2017.

37 Anna Costanza Baldry et al. "Cyberbullying and Cybervictimization versus Parental Supervision, Monitoring and Control of Adolescents' Online Activities", Children and Youth Services Review, 2019.

38 The Luxembourg Guidelines, 2016 and the UNICEF Global Kids Online report, 2019 (as above).

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"[39].

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[40].

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[41]. 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. Он также связан с эмоциональным интеллектом, необходимым для того, чтобы понимать, когда ребенок подвергается риску в интернете, знать, как обращаться за помощью, извлекать практические уроки и восстанавливаться после неудачного опыта[42].

Руководители

Относится ко всем лицам, занимающим должности в школьном руководстве или руководящих структурах.

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*". Это уголовно наказуемое деяние, в рамках которого заводится дружба с ребенком ... с целью склонить его к сексуальным отношениям.

Информационно-коммуникационные технологии

Информационно-коммуникационные технологии (ИКТ) 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 консоли и "умные" часы[43]. Сюда же относятся услуги, например радио и телевидение, широкополосная связь, сетевое оборудование и спутниковые системы.

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

---

39 UNICEF Global Kids Online report, 2019 (as above).
40 Council of Europe, "Digital Citizenship and Digital Citizenship Education".
41 Western Sydney University, "What is digital literacy?".
42 Dr. Andrew K. Przybylski, et al., "A Shared Responsibility: Building children's' online resilience", Virgin Media and Parent Zone, 2014.
43 ЮНИСЕФ и МСЭ "Руководящие указания для отрасли по защите ребенка в онлайновой среде", 2014 г. (см. выше).

видеоматериалами, которые обычно предусматривают для зрителей возможность оставлять комментарии или общаться с игроками и другими представителями аудитории[44].

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[45].

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 означают 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 и осознания важности сохранения конфиденциальности[46].

Общественные средства массовой информации

К ним относятся национальные радиовещательные организации или средства массовой информации, получившие лицензию на радиовещание на основании ряда договорных обязательств, согласованных с государством или парламентом. В последнее время во многих странах такие обязательства были дополнены с учетом необходимости реагировать на последствия цифровой трансформации с помощью средств массовой информации и цифровых программ повышения грамотности и обязанностей по устранению цифрового разрыва.

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[47]. В большинстве стран создание, распространение и хранение изображений детей сексуального характера является незаконным. В случае распространения собственноручно созданных изображений детей сексуального характера взрослые не должны просматривать их. Демонстрация изображений сексуального характера ребенку взрослым всегда представляет собой преступное деяние, способное нанести вред, и возможно потребуется сообщить о таких изображениях или устранить их.

Секс-вымогательство, или сексуальное вымогательство в отношении детей

Сексуальное вымогательство 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)"[48].

---

44 UNICEF, "Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry", 2019.
45 ЮНИСЕФ и МСЭ "Руководящие указания для отрасли по защите ребенка в онлайновой среде", 2014 г. (см. выше).
46 US Federal Trade Commission, "Children's Online Privacy Protection Act", 1998.
47 The Luxembourg Guidelines, 2016 (as above).
48 The Luxembourg Guidelines, 2016 (as above).

Интернет вещей

"Интернет вещей (IoT) является следующим шагом в направлении цифровизации нашего общества и экономики, когда взаимосвязь людей и объектов осуществляется через коммуникационные сети, а также передаются сведения об их состоянии и окружающей обстановке"[49].

URL

Сокращение, означающее "универсальный указатель ресурса" ("Uniform Resource Locator"), т. е. адрес страницы в интернете[50] .

Виртуальная реальность

"Виртуальная реальность – это создание при помощи компьютерных технологий эффекта трехмерного мира, в котором объекты воспринимаются как реально существующие в пространстве"[51].

Wi-Fi

Wi-Fi (от англ. "Wireless Fidelity" – "высокая точность беспроводной передачи") – набор технических стандартов, обеспечивающих возможность передачи данных по беспроводным сетям[52].

49 European Commission, "Policy: The Internet of Things".
50 ЮНИСЕФ и МСЭ "Руководящие указания для отрасли по защите ребенка в онлайновой среде", 2014 г. (см. выше).
51 NASA, "Virtual Reality: Definition and Requirements".
52 US Federal Trade Commission, "Children's Online Privacy Protection Act", 1998.

With the support of:

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

ISBN: 978-92-61-30414-0

Опубликовано в Швейцарии
Женева, 2020 г.

Фотографии представлены: Shutterstock