НАБОР ПРОГРАММНЫХ СРЕДСТВ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДЕТЕЙ В ИНТЕРНЕТЕ

РЕАЛЬНЫЕ ИНСТРУМЕНТЫ ДЛЯ ЗАЩИТЫ ДЕТЕЙ В ИНТЕРНЕТЕ

5RIGHTS FOUNDATION

End Violence Against Children

О Фонде 5Rights

Цифровой мир, которого заслуживает молодое поколение

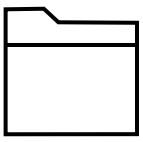
5Rights разрабатывает новую политику, инновационные структуры и технические стандарты, публикует исследования, решает проблемы и следит за тем, чтобы права и потребности детей признавались и приоритезировались в цифровой среде.

Мы концентрируемся на реальных изменениях, и результаты нашей работы цитируются и широко используются во всем мире. Мы сотрудничаем с правительствами, межгосударственными организациями, профессиональными ассоциациями, научными кругами, предприятиями, НПО и детьми. Всё это направлено на то, чтобы цифровые продукты и услуги оказывали положительное влияние на жизнь молодого поколения. По определению Конвенции Организации Объединенных Наций о правах ребенка, детьми считаются лица, не достигшие 18-летнего возраста.

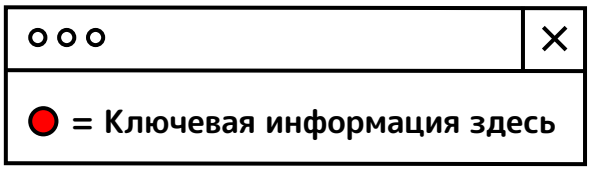
Данная публикация подготовлена при финансовой поддержке Фонда по борьбе с насилием в отношении детей в рамках его инициативы «Безопасность в Интернете» (Safe Online). Фонд по борьбе с насилием оказывает финансовую поддержку программам, которые предлагают практические, новаторские решения для защиты детей от эксплуатации и злоупотребления их правами в Интернете Мнения, выводы, заключения и рекомендации Фонда 5Rights, содержащиеся в настоящем документе, не обязательно совпадают с точкой зрения Фонда по борьбе с насилием в отношении детей.

5RIGHTS FOUNDATION

End Violence Against Children



Содержание



ПРЕДИСЛОВИЕ

«В этот беспрецедентный момент нельзя недооценивать мощь, преимущества и опасность цифровых технологий. Объединение усилий позволит международному сообществу добиться того, чтобы технологии использовались во благо и были доступны всем, а также найти способы управлять их воздействием.

Судить о том, смогли ли мы использовать все возможности эпохи цифровых взаимосвязей, будет будущее поколение. Сейчас пришло время действовать».

Антониу Гутерриш,
Генеральный секретарь Организации Объединенных Наций
План мероприятий Генерального секретаря по цифровому сотрудничеству, июнь 2020 г.

ПРЕДИСЛОВИЕ

«Мы не сможем построить устойчивое будущее, если не в состоянии создать детям безопасные и защищенные от насилия и вреда условия, в том числе в цифровой среде. Несмотря на то, что все мы имеем примерное представление о том, каким должен быть цифровой мир для детей, всё становится гораздо сложнее, когда мы начинаем воплощать эти принципы безопасности и доступности в реальную политику, законы, действия, а также продукты и услуги.

Надеемся, что Набор программных средств для обеспечения безопасности детей в Интернете, представляющий собой практическое руководство для законодателей, поможет решить ключевые вопросы, касающиеся защиты детей в цифровой среде».

Д-р Говард Тейлор,
исполнительный директор
Фонда по борьбе с насилием в отношении детей

СИСТЕМНАЯ ПАПКА

8 ДОКУМЕНТОВ | 105 МБ НА ДИСКЕ | РАЗДЕЛ 1

СЛЕДУЮЩИЙ РАЗДЕЛ >

Введение

В мире, всё более наполненном технологиями, потребность в безопасной и благоприятной цифровой среде для детей велика как никогда. Законодатели во всем мире работают над созданием правил взаимодействия детей с цифровым миром. Наибольшее внимание этой проблеме уделено в Плане мероприятий по цифровому сотрудничеству Генерального секретаря ООН.[1] Данный Набор программных средств для обеспечения безопасности детей в Интернете является инструментом поддержки законодателей и специалистов-практиков, предлагающий доступный, практический подход к построению цифрового мира, который учитывает интересы детей, благоприятно влияя на их жизнь как в Интернете, так и за его пределами.

Данный Набор программных средств содержит план мероприятий, необходимых для обеспечения безопасности и соблюдения прав детей в цифровом мире. Все обязательства разделены на десять тематических областей, способствующих реализации следующих ключевых международных соглашений и рамочных программ: Цели устойчивого развития (ЦУР); замечание общего порядка № 25 (2021) КПР ООН о правах ребенка в цифровой среде; Модель национального реагирования Глобального альянса WeProtect и Руководящие принципы по защите детей в Интернете Международного союза электросвязи.

Данный Набор программных средств не призван заменить собой какие-либо существующие региональные, национальные или международные соглашения или рамочные программы. Он содержит примеры передовой практики со всего мира, служит ориентиром для создания детальных подходов к каждому аспекту политики и определяет меры, которые необходимо предпринять отдельным лицам и группам специалистов, на которых возложена задача по обеспечению безопасности детей в Интернете. По сути, это инструмент поддержки законодателей со всего мира, объединяющий обязательства, которые уже на них возложены.

Гарантия безопасности в Интернете — это не только предотвращение рисков и вреда, но и активное создание цифровой среды, безопасной для каждого ребенка. Поскольку каждый третий человек в возрасте до 18 лет использует Интернет, очевидно центральное место цифровых технологий в жизни ребенка. Это значит, что в них должны быть встроены конфиденциальность, безопасность и права детей. Именно такой превентивный и целостный подход отражен в данном Наборе программных средств, содержащем план мероприятий по разработке, оценке и совершенствованию политик и практик в отношении прав детей на уровне правительств, государств и организаций. Он позволит всем ответственным лицам внести свой вклад в создание глобального подхода к обеспечению безопасности детей в Интернете, который будет со временем эволюционировать. Данный Набор программных средств предназначен для использования законодателями во всем мире, в том числе в странах, недавно получивших доступ к Интернету, и может быть адаптирован в различные контекстах и условиях.

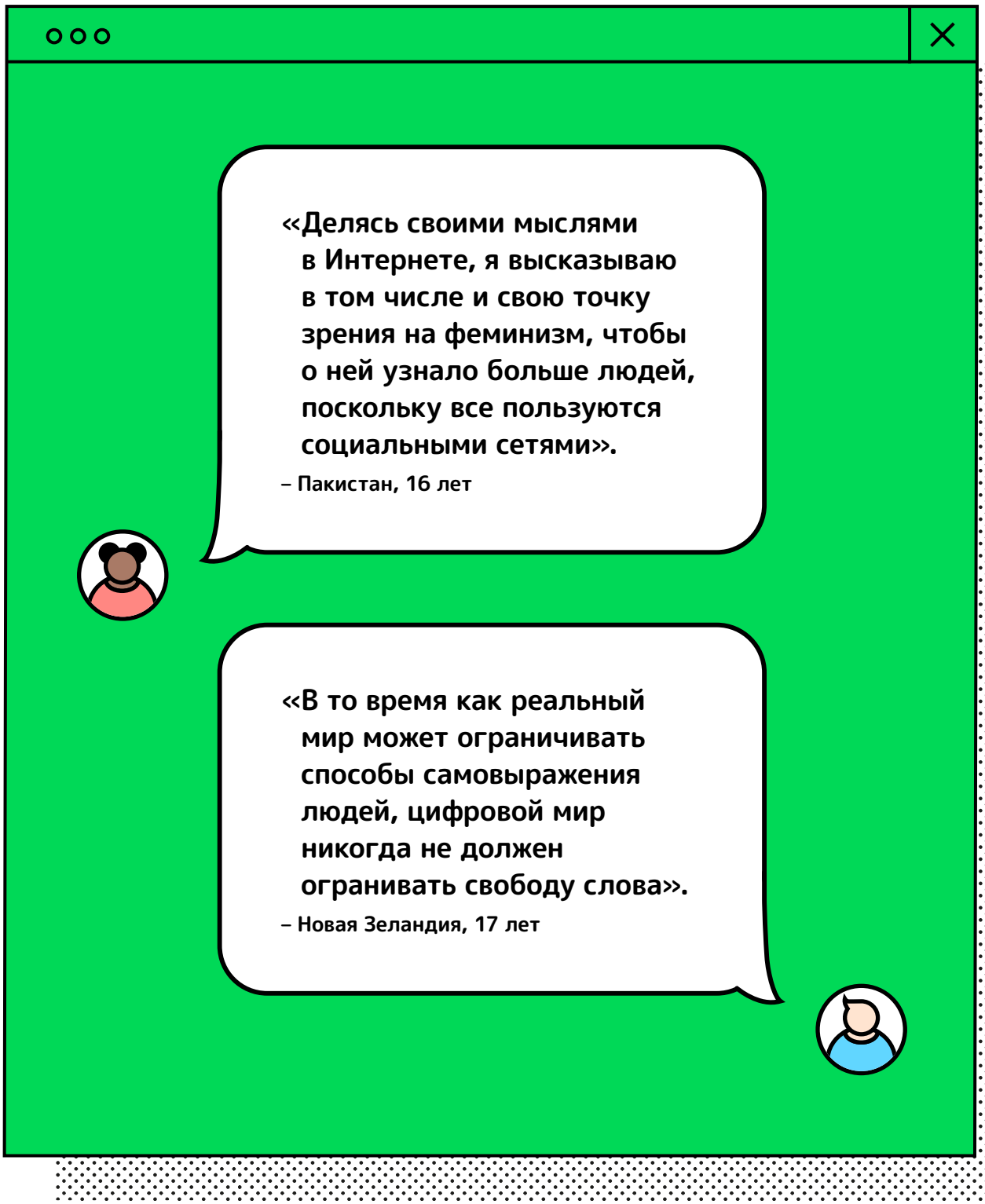
От лица 5Rights и нашего сообщества хочу поблагодарить Генерального секретаря *Антониу Гутерриша* за его дальновидные руководящие усилия по разработке плана мероприятий для построения цифрового мира и за признание того, что без обеспечения безопасности и соблюдения прав детей в эпоху интернета мы не сможем построить лучший мир для всех. Необходимо также отметить, что первоначальная работа, на которой основан данный Набор программных средств, была проделана по поручению правительства Руанды. Мы признательны за поддержку, благодаря которой смогли использовать результаты этой работы в настоящем проекте. Мы также выражаем благодарность кавалеру Ордена Британской империи профессору Джулии Дэвидсон и доктору Сьюзи Алегре за их вклад в подготовку данного документа. Кроме того, мы хотели бы отметить щедрую поддержку Фонда по борьбе с насилием в отношении детей, который помог нам разработать Политику обеспечения безопасности детей в Интернете для правительства Руанды и впоследствии нашел возможность превратить ее в документ, который может принести пользу всем странам.

При работе над структурой и содержанием данного Набора программных средств мы опирались на работу многих других организаций. к их числу относятся, в частности, Комитет ООН по правам ребенка, Глобальный альянс WeProtect, Фонд по борьбе с насилием в отношении детей, Университет Восточного Лондона, Университет Руанды, Фонд 5Rights и многие другие государства, глобальные межправительственные организации, академические круги, сообщества по защите детей и правоохранительной деятельности. Мы выражаем им свою признательность и благодарность за их труд, приверженность своему делу и внесенный вклад. Но, прежде всего, своим подходом этот документ обязан сотням детей и молодых людей, которые рассказали нам, что хотят взаимодействовать с цифровым миром творчески, безопасно и безбоязненно. Этот Набор программных средств создан с их помощью и для них.

Баронесса Бибан Кидрон, кавалер Ордена Британской империи,
основатель и председатель Фонда 5Rights

1. План мероприятий Генерального секретаря Организации Объединенных Наций по цифровому сотрудничеству, Организация Объединенных Наций, 2020 г.

СЛЕДУЮЩИЙ РАЗДЕЛ >



СИСТЕМНАЯ ПАПКА

8 ДОКУМЕНТОВ | 105 МБ НА ДИСКЕ | РАЗДЕЛ 2

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

Инструкция пользователя

Набор программных средств для обеспечения безопасности детей в Интернете представляет собой практический инструментарий, помогающий законодателям во всем мире выполнять свои международные обязательства в отношении прав детей и безопасности детей в Интернете.

Для одних этот документ послужит отправной точкой, другим он даст возможность сопоставить их нынешнюю политику и ее реализацию с передовой международной практикой. Он разработан безотносительно к конкретной стране с тем, чтобы законодатели, проводя анализ своего национального контекста, могли использовать его для оценки и обоснования своего собственного пути к включению прав детей в цифровую среду.

Набор программных средств включает:

- Всеобъемлющую и надежную «типовую» политику по обеспечению безопасности детей в Интернете как один из подходов, который законодатели могут применять или развивать для обеспечения эффективной координации между юрисдикциями.
- Десять направлений деятельности для законодателей по разработке собственной политики безопасности детей в Интернете.
- Контрольные списки и другие инструменты аудита, которые законодатели могут использовать для оценки и совершенствования текущих и планируемых мер в своей стране по обеспечению безопасности детей в Интернете.
- Краткое изложение глобальных основополагающих документов и руководящие принципы к ним.
- Глоссарий ключевых терминов, используемых в сфере безопасности в Интернете и политике безопасности детей в Интернете.
- Примеры передовой практики и информация из различных стран.
- Диаграммы и другие пояснительные материалы, помогающие донести идеи политики до других аудиторий, включая государственных служащих и гражданское общество.

Разработка Набора программных средств — это ответ на призыв Генерального секретаря ООН к действию в рамках его Дорожной карты цифрового сотрудничества (2020 г.), объединяя основополагающие ресурсы: Замечание общего порядка № 25 (2021 г.) КПР ООН, Руководящие принципы по защите детей в Интернете Международного союза электросвязи и Модель национального реагирования Глобального альянса WeProtect, чтобы предоставить практический ресурс законодателям по обеспечению безопасности детей в Интернете.

Набор программных средств и его ресурсы доступны в Интернете по адресам childonlinesafetytoolkit.org и info@5rightsfoundation.com.

Язык имеет значение. Слова, которые мы используем, влияют на то, что мы думаем о правах детей и их безопасности в Интернете. Слова, которые мы употребляем, влияют на то, как мы расставляем приоритеты в вопросах, как реагируем, а также, что немаловажно, на нашу способность эффективно сотрудничать и обеспечивать или соблюдать права детей в разных странах. Хотя условия в каждой стране могут быть разными, крайне важно, чтобы законы и нормативные акты в максимально возможной степени использовали концепции, формулировки и определения, которые согласованы и позволяют наладить сотрудничество между правоохранительными органами, а также международное сотрудничество и взаимопонимание в более широком смысле.[2] Набор программных средств включает признанные на международном уровне глоссарии Комитета Организации Объединенных Наций по правам детей и Люксембургские руководящие принципы, которые помогают создать шаблоны для используемого языка.[3]

Этот Набор программных средств дополняет и подчеркивает уже хорошо разработанные модели для поддержки конкретных аспектов безопасности детей в Интернете.

К основным ресурсам относятся:

- Замечание общего порядка № 25 (2021 г.) о правах детей в отношении цифровой среды, которое является важнейшим инструментом для понимания прав детей в контексте безопасности детей в Интернете. в нем Комитет ООН по правам ребенка разъясняет, каким образом государства должны выполнять Конвенцию о правах ребенка в отношении цифровой среды и дает рекомендации в отношении соответствующих законодательных, политических и других мер для обеспечения полного соблюдения их обязательств по Конвенции и Факультативным протоколам.[4]
- *Модель национального реагирования* (MNR) Глобального альянса WeProtect имеет особое значение в проблеме сексуальной эксплуатации детей и жестокого обращение с ними (CSEA). MNR является ключевым элементом любого национального инструментария для обеспечения безопасности детей в Интернете.[5] MNR нацелена на оказание помощи странам в разработке мер реагирования на сексуальную эксплуатацию детей и жестокое обращение с ними в Интернете, однако в ней подчеркивается, что данную проблему нельзя решать изолированно, и заявляется, что для обеспечения полномасштабных мер национального реагирования необходим более широкий набор возможностей по предотвращению и пресечению сексуальной эксплуатации детей и жестокого обращения с ними. в данном Наборе программных средств представлены ресурсы, способствующие реализации MNR. Набор программных средств для обеспечения безопасности детей в Интернете может помочь сторонам, подписавшим MNR Глобального альянса WeProtect, убедиться в том, что они обладают институциональным потенциалом для реализации его целей и выполнения обязательств по Замечаниям общего порядка.
- *Руководящие принципы Международного союза электросвязи (МСЭ) по безопасности детей в Интернете* 2020 представляют собой всеобъемлющий набор рекомендаций и инструментов для всех соответствующих заинтересованных сторон в отношении того, как помочь созданию безопасной Интернет-среды, которая способствует расширению прав и возможностей детей и молодежи. Они предназначены для четырех основных аудиторий: детей, родителей/опекунов и педагогов, представителей отрасли и законодателей. Для каждой из этих аудиторий руководящие принципы призваны служить в качестве образца, который можно адаптировать и использовать в соответствии с национальными или местными обычаями и законами, а также решать вопросы, которые могут затрагивать всех детей и молодых людей в возрасте до 18 лет.[6]

2. «Комитет рекомендует странам-участницам при разработке своей правовой базы принимать во внимание технологические достижения, чтобы обеспечить применимость такой базы с учетом будущего технологического прогресса, а также во избежание лазеек, связанных с вновь возникающими проблемами, включая новые формы торговли людьми в Интернете и сексуальной эксплуатации. с учетом меняющегося характера данной проблемы государства-участники должны регулярно оценивать и, при необходимости, пересматривать свои законодательства и политики, чтобы гарантировать адаптацию своих правовых и политических норм к быстро меняющимся реалиям». Руководящие принципы, касающиеся реализации Факультативного протокола в рамках Конвенции о правах ребенка в части противодействия торговле детьми, детской проституции и детской порнографии, Комитет ООН по правам ребенка, 2019 г.
3. Универсальная терминология: Терминологическое руководство по защите детей от сексуальной эксплуатации и сексуального насилия, ECPAT International, 2016 г.
4. Противодействие сексуальной эксплуатации детей и жестокому обращению с ними (CSEA): Модель национального реагирования, Глобальный альянс WeProtect, 2015.
5. Замечание общего порядка № 25 о правах детей в отношении цифровой среды, Конвенция ООН о правах ребенка, 2021 г.
6. Руководящие принципы по защите детей в Интернете, Международный союз электросвязи, 2020 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

К числу других важных ресурсов и рамок, имеющих значение для законодателей, занимающихся вопросами безопасности детей в Интернете, относятся:

- **ООН**: ***Цели устойчивого развития.*** 17 Целей устойчивого развития (ЦУР) лежат в основе Повестки дня в области устойчивого развития на период до 2030 года,[7] принятой всеми государствами-членами Организации Объединенных Наций в 2015 году.
- **ООН**: ***Руководящие принципы предпринимательской деятельности в аспекте прав человека*** .[8] Эти принципы устанавливают обязательства государств-участников и предприятий по защите и соблюдению прав человека, включая права детей.
- **Программа Всемирной организации здравоохранения *INSPIRE: семь стратегий по искоренению насилия в отношении детей.***[9] INSPIRE — это разработанный на фактических материалах технический пакет для поддержки действий государств-участников по предотвращению насилия в отношении детей и реагированию на него.
- **ЮНИСЕФ: *Проект Руководства по созданию политики в области искусственного интеллекта для детей.***[10] Руководство предназначено для продвижения прав детей в политике и практике применительно к искусственному интеллекту в государственном и частном секторе, а также для повышения осведомленности о том, как системы ИИ могут поддерживать реализацию этих прав или препятствовать ей.

Существует множество других подобных документов на региональном, национальном и международном уровне, которые могут быть актуальны для конкретных стран или обеспечивать глобально значимые модели, многие из которых приведены в соответствующих разделах данного Набора программных средств.

Распространенность сексуальной эксплуатации детей и жесткого обращения с ними также вызывает серьезную озабоченность. в 2020 году в Национальный центр по проблемам пропавших и подвергающихся эксплуатации детей поступило 65 миллионов материалов по сексуальным надругательствам над детьми, однако гораздо большее количество подобных случаев остаются невыявленными.[11] Международное сообщество давно сплотилось в общей решимости защищать детей. На основе этой решимости расширилось сотрудничество между национальными правоохранительными органами и крупными технологическими компаниями, однако можно сделать еще больше.

Компании должны внедрить более надежные технологии поиска и ускорить методы обнаружения, ориентированные на предотвращение негативных явлений в этой сфере. Этот подход должен также подкрепляться важными шагами в области законодательства. в этой связи большое значение имеют многосторонние партнерства с участием таких заинтересованных сторон, как Глобальный альянс WeProtect и Глобальное партнерство за искоренение насилия в отношении детей.

Источник: План мероприятий Генерального секретаря ООН по цифровому сотрудничеству, июнь 2020[12]

7. Преобразование нашего мира: Повестка дня в области устойчивого развития на период до 2030 года, Организация Объединенных Наций, 2021 г.
8. Руководящие принципы предпринимательской деятельности в аспекте прав человека, Управление Верховного комиссара Организации Объединенных Наций по правам человека, 2011 г.
9. Программа INSPIRE: семь стратегий по искоренению насилия в отношении детей, Всемирная организация здравоохранения, 2021 г.
10. Руководство по созданию политики в области искусственного интеллекта для детей, Детский фонд Организации Объединенных Наций, 2020 г.
11. Отчет CyberTipline, Национальный центр по проблемам пропавших и подвергающихся эксплуатации детей, 2020 г.
12. План мероприятий Генерального секретаря Организации Объединенных Наций по цифровому сотрудничеству, Организация Объединенных Наций, июнь 2020 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

Как мы сделали это

Цифровой мир постоянно меняется. Политика обеспечения безопасности детей в Интернете должна основываться на подходе, основанном на правах ребенка, и быть достаточно гибкой, чтобы соответствовать меняющимся возможностям и рискам по мере их возникновения. Набор программных средств для обеспечения безопасности детей в Интернете предназначен для удовлетворения этой потребности и предоставляет для этого всеобъемлющий набор мер по разработке приемлемой политики, примеры передовой практики и ресурсы для общего использования.

Данный Набор программных средств является продуктом консультаций в мировом масштабе, в нем учтены мнения со всех континентов и территорий, начиная от малых островных развивающихся государств и заканчивая крупными промышленными странами, а также включая все, что находится между ними.[13] Мы провели консультации с международными экспертами из различных сфер деятельности, включая предпринимателей, законодателей и ученых. Данный проект был подготовлен Фондом 5Rights, штаб-квартира которого находится в Великобритании, при поддержке коллег из Европы, Северной Америки и Австралии, а также партнеров[14], которые проводили фокус-группы в Латинской Америке, Африке и Азии, чтобы обеспечить практичность и актуальность Набора программных средств с учетом особенностей разных стран. Этот текст основан на глобальных стандартах, в частности, на Конвенции ООН о правах ребенка, однако Набор программных средств также может быть адаптирован для отражения культур и ценностей, закрепленных в национальных конституциях по всему миру.

Это целостный, практичный и доступный инструментарий для законодателей, призванный проложить путь к миру, в котором все дети будут чувствовать себя в безопасности и в полной мере реализованными, – миру, в котором полностью соблюдаются их права как в Интернете, так и за его пределами.

В ходе консультаций дети высказали мнение о том, что цифровая среда должна поддерживать, поощрять и защищать их безопасное и равноправное участие:

«Мы бы хотели, чтобы правительство, технологические компании и учителя помогали нам научиться распознавать недостоверную информацию в Интернете».
– Гана, возраст неизвестен

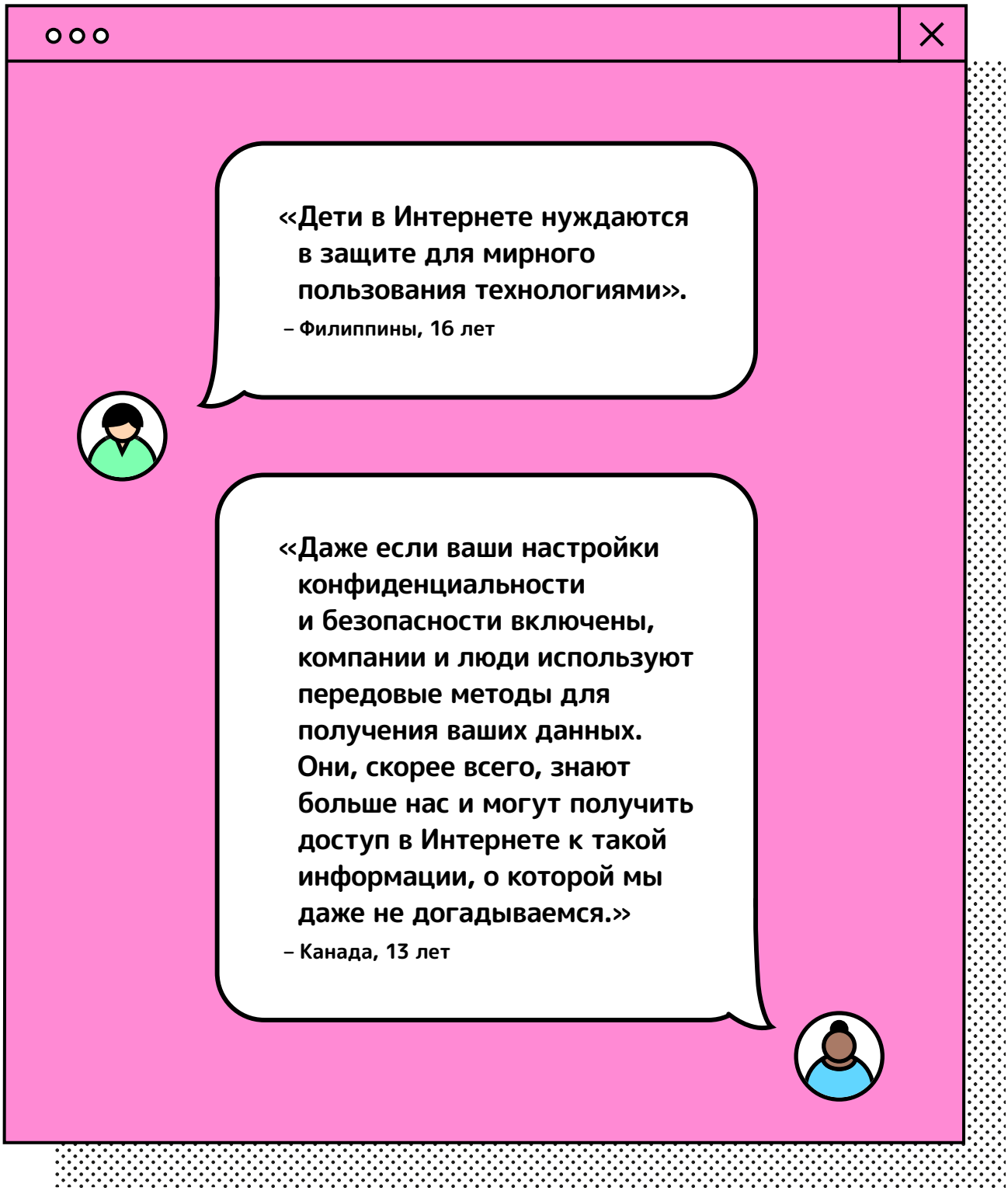
«Я хотел бы ясно понимать, что на самом деле происходит с моими данными… Зачем их собирают? Как их собирают?»
– Германия, 16 лет

«Я… переживаю, что мои данные могут быть кому-то переданы».
– Канада, 15 лет

13. Включая опросы целевых групп в Бразилии, Гане, Зимбабве, Камбодже, Колумбии и Шри-Ланке для обеспечения глобальной применимости.
14. Партнеры из стран-участниц были представлены следующими организациями: RedPapaz из Колумбии, Alana Foundation из Бразилии, African Digital Rights Hub из Ганы, UNICEF Zimbabwe, UNICEF Cambodia и Save the Children International из Шри-Ланки.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >



СИСТЕМНАЯ ПАПКА

8 ДОКУМЕНТОВ | 105 МБ НА ДИСКЕ | РАЗДЕЛ 3

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

Важность соблюдения прав детей

Права детей являются неотъемлемой частью любой политики, затрагивающей жизнь детей как в Интернете, так и за его пределами. Цель политики обеспечения безопасности детей в Интернете, по сути, заключается в том, чтобы право детей на защиту и участие было реальным и эффективным в процессе их взаимодействия с цифровым миром.

Права детей и их семей закреплены в Международном билле о правах, включая Всеобщую декларацию прав человека 1948 года, Международный пакт о гражданских и политических правах 1966 года и Международный пакт об экономических, социальных и культурных правах 1966 года, а также в региональных и национальных структурах по правам человека.

Что касается конкретно детей, то *Конвенция Организации Объединенных Наций о правах ребенка 1989 года* («Конвенция» или КПР)[15] вместе с *Факультативными протоколами к ней, касающимися вопросов торговли детьми*[16] *и участия детей в вооруженных конфликтах,*[17] обеспечивают практическую основу для понимания того, как права человека применяются к детям. Конвенция — это договор по правам человека, который ратифицировали наибольшее количество государств в истории, а Факультативный протокол к ней, касающийся процедуры сообщений, помогает обеспечить ее исполнение с тем, чтобы права детей имели реальное применение и юридическую силу.

Все права, содержащиеся в КПР, направлены на безопасность детей в Интернете, в то время как консультации с детьми имеют решающее значение для понимания того, что эти права означают на практике. Например, следует рассмотреть вопрос о правах детей на игру, участие и семейную жизнь в онлайн-пространстве. Все, кто участвует в проведении консультаций, должны пройти надлежащую подготовку по вопросам прав детей, учета мнений детей и их вовлечения в жизнь общества.

В Замечании общего порядка № 25 (2021) *Комитет Организации Объединенных Наций по правам ребенка*[18] дает руководящие указания относительно законодательных, политических и других соответствующих мер для обеспечения полного соблюдения обязательств по Конвенции и Факультативным протоколам к ней в свете возможностей, рисков и проблем, связанных с правами детей в цифровой среде. Замечание общего порядка № 25 (2021) станет ключевым инструментом, который следует учитывать при разработке политики в области безопасности детей в Интернете.

> **Права каждого ребенка должны соблюдаться, защищаться и реализовываться в цифровой среде. Инновации в области цифровых технологий влияют на жизнь детей и их права широкомасштабно и взаимозависимо, даже если сами дети не имеют доступа к Интернету. Разумный доступ к цифровым технологиям может помочь детям реализовать весь спектр своих гражданских, политических, культурных, экономических и социальных прав. Однако если цифровая интеграция не будет достигнута, существующее неравенство, скорее всего, углубится и могут возникнуть новое неравенство.**
>
> Источник: Замечание общего порядка № 25 (2021), пункт 4[19]

15. Конвенция о правах ребенка, Управление Верховного комиссара Организации Объединенных Наций по правам человека, 1989 г.
16. Конвенция о правах ребенка, Управление Верховного комиссара Организации Объединенных Наций по правам человека, 1989 г.
17. Конвенция о правах ребенка, Управление Верховного комиссара Организации Объединенных Наций по правам человека, 1989 г.
18. Замечание общего порядка № 25 (2021 год) о правах детей в отношении цифровой среды, Комитет Организации Объединенных Наций по правам ребенка, 2021 г.
19. Замечание общего порядка № 25 (2021 год) о правах детей в отношении цифровой среды, Комитет Организации Объединенных Наций по правам ребенка, 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

КПР дает четыре руководящих принципа защиты прав детей, а Замечание общего порядка № 25 (2021) описывает, как они применяются в цифровом мире:

1. Право на свободу от дискриминации (статья 2)

Статья 2 Конвенции о правах ребенка[20] гласит, что каждый ребенок имеет право пользоваться своими правами в равной степени, «без какой бы то ни было дискриминации, независимо от расы, цвета кожи, пола, языка, религии, политических или иных убеждений, национального, этнического или социального происхождения, имущественного положения, инвалидности, рождения или иного обстоятельства ребенка или его родителей или законных опекунов». в пунктах 10 и 11 Замечания общего порядка № 25 (2021) описывают, как это применимо в цифровом мире.

> **Дети могут подвергаться дискриминации в силу того, что они лишены возможности пользоваться цифровыми технологиями и услугами, или в силу того, что получают ненавистнические сообщения или подвергаются несправедливому обращению в результате использования этих технологий. Другие формы дискриминации могут возникать в тех случаях, когда автоматизированные процессы, в результате которых происходит отбор информации, составление профиля или принятие решений, основаны на предвзятых, частичных или несправедливо полученных данных о ребенке.**
>
> **Комитет призывает государства-участники принимать активные меры по предотвращению дискриминации по признаку пола, инвалидности, социально-экономического положения, этнического или национального происхождения, языка или по любым другим признакам, а также дискриминации в отношении детей из числа меньшинств и коренных народов, детей-просителей убежища, детей-беженцев и детей-мигрантов, детей-лесбиянок, детей-геев, детей-бисексуалов, детей-трансгендеров и детей-интерсексуалов, детей, ставших жертвами торговли людьми или сексуальной эксплуатации, детей, находящихся на альтернативном попечении, детей, лишенных свободы, и детей, находящихся в ином уязвимом положении. Потребуются конкретные меры для устранения гендерного цифрового разрыва для девочек, в которых особое внимание уделялось бы доступу, компьютерной грамотности, конфиденциальности и безопасности в Интернете.**
>
> Источник: Замечание общего порядка № 25 (2021), пункты 10-11[21]

20. Конвенция о правах ребенка, Управление Верховного комиссара Организации Объединенных Наций по правам человека, ООН, 1989 г.
21. Замечание общего порядка № 25 (2021 год) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

2. Наилучшее обеспечение интересов ребенка (пункт 1 статья 3)

Статья 3 Конвенции о правах ребенка[22] гласит, что «во всех действиях в отношении детей, независимо от того, предпринимаются ли они государственными или частными учреждениями социального обеспечения, судами, административными или законодательными органами, первоочередное внимание уделяется наилучшему обеспечению интересов ребенка». в пунктах 12 и 13 Замечания общего порядка № 25 (2021) описывают, как это применимо в цифровом мире.

Наилучшие интересы ребенка – это динамичная концепция, которая требует оценки, соответствующей конкретному контексту. Цифровая среда изначально не была предназначена для детей, однако сегодня она играет важную роль в их жизни. Государства-участники должны создать необходимые условия, при которых во всех действиях, касающихся обеспечения, регулирования, разработки, управления и использования цифровой среды первоочередное внимание уделялось бы наилучшему обеспечению интересов каждого ребенка.

Государства-участники должны привлекать к таким действиям национальные и местные органы, которые следят за реализацией прав детей. При рассмотрении вопроса о наилучших интересах ребенка они должны учитывать все права детей, включая их право на поиск, получение и распространение информации, на защиту от вреда и на то, чтобы их мнению уделялось должное внимание, а также на обеспечение прозрачности оценки наилучших интересов ребенка и применяемых при ней критериев.

Источник: Замечание общего порядка № 25 (2021), пункты 12-13[23]

3. Право на жизнь, выживание и развитие (статья 6)

Статья 6 Конвенции о правах ребенка[24] требует, чтобы государства-участники «признавали, что каждый ребенок имеет неотъемлемое право на жизнь» и что они должны «в максимально возможной степени обеспечить выживание и развитие ребенка». в пункте 15 Замечания общего порядка № 25 (2021) описывают, как это применимо в цифровом мире.

Использование цифровых устройств не должно быть во вред ребенку и не должно подменять собой личные контакты между детьми или между детьми и родителями или опекунами. Государства-участники должны уделять особое внимание воздействию технологий в первые годы жизни ребенка, когда пластичность мозга максимальна, а социальная среда, в частности, отношения с родителями и опекунами, имеет решающее значение для когнитивного, эмоционального и социального развития ребенка. в первые годы может потребоваться принятие мер предосторожности в зависимости от назначения, цели и применения технологий. Родители, опекуны, педагоги и другие привлеченные лица должны проходить профессиональное обучение и получать консультирование по надлежащему использованию цифровых устройств с учетом результатов исследований о влиянии цифровых технологий на развитие детей, особенно в период критического неврологического всплеска роста в раннем детстве и подростковом возрасте.

Источник: Замечание общего порядка № 25 (2021 г.), пункт 15[25]

22. Конвенция о правах ребенка, Управление Верховного комиссара Организации Объединенных Наций по правам человека, ООН, 1989 г.
23. Замечание общего порядка № 25 (2021 год) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.
24. Конвенция о правах ребенка, Управление Верховного комиссара Организации Объединенных Наций по правам человека, ООН, 1989 г.
25. Замечание общего порядка № 25 (2021 год) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

4. Право быть выслушанным (статья 12):

Статья 12 Конвенции о правах ребенка[26] требует от государств-участников обеспечить условия, при которых дети в тех случаях, когда они «способны формировать (свои) собственные взгляды», пользовались бы «правом свободно выражать эти взгляды по всем затрагивающим (их) вопросам», и уделять этим взглядам «должное внимание в соответствии с возрастом и зрелостью ребенка». в пункте 17 Замечания общего порядка № 25 (2021) изложено, как это применяется в цифровом мире, а дополнительную информацию о том, как реализовать это право, можно найти в Ресурсах 1 ниже.

> **При разработке законопроектов, политик, программ, услуг и профессионального обучения по правам детей относительно цифровой среды государства-участники должны учитывать всех детей, прислушиваться к их потребностям и уделять должное внимание их взглядам. Они должны обеспечить условия, при которых поставщики цифровых услуг будут активно взаимодействовать с детьми, применяя соответствующие меры предосторожности и должным образом учитывать их мнение при разработке продуктов и услуг.**
>
> Источник: Замечание общего порядка № 25 (2021), пункт 17 [27]

Эти принципы неразделимы и должны учитываться при разработке политики безопасности детей в Интернете. Они представляют собой полезную «линзу», через которую можно рассмотреть, что на самом деле означают на практике остальные пять межсекторальных вопросов и как следует осуществлять деятельность в десяти областях применения политики, обозначенных в Наборе программных средств.

Права детей закреплены не только в международном праве. Большинство мировых конституций или нормативно-правовых актов содержат общие положения о правах человека, защищающие детей. Эти национальные законы о правах человека также следует использовать при разработке политики безопасности детей в Интернете, которая ставит во главу угла защиту и продвижение прав детей.

Комитет ООН по правам ребенка призывает государства обеспечить такие условия, при которых в национальной политике, касающейся прав детей, особое внимание уделялось бы цифровой среде и защита детей в Интернете была интегрирована в национальную политику защиты детей. Данный Набор программных средств призван помочь им в этом.

26. Конвенция о правах ребенка, Управление Верховного комиссара Организации Объединенных Наций по правам человека, ООН, 1989 г.
27. Замечание общего порядка № 25 (2021 год) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

Государства-участники должны обеспечивать такие условия, при которых национальная политика в отношении прав детей конкретно касалась бы цифровой среды, и внедрять соответствующие нормативные акты, отраслевые кодексы, нормы проектирования и планы действий, которые должны регулярно оцениваться и обновляться. Их национальная политика должна обеспечивать предоставление детям возможности получать пользу от цифрового окружения и гарантировать безопасный доступ к нему.

Защита детей в Интернете должна была интегрирована в национальную политику защиты детей. Государства-участники должны осуществлять меры по защите детей от рисков, включая кибер-агрессию и сексуальную эксплуатацию детей и жестокое обращение с ними в Интернете и с помощью цифровых технологий, обеспечивать расследование таких преступлений и предоставлять средства правовой защиты и поддержку детям, ставшим жертвами таких преступлений. Они должны также учитывать потребности детей, находящихся в неблагоприятном или уязвимом положении, в том числе путем предоставления ориентированной на детей информации, которая при необходимости должна быть переведена на соответствующие языки меньшинств.

Государства-участники должны обеспечить наличие эффективных механизмов защиты детей в Интернете и осуществлять политику обеспечения безопасности без ущерба для других прав детей в любых местах, где дети имеют доступ к цифровой среде, включая дом, образовательные учреждения, киберкафе, молодежные центры, библиотеки, учреждения здравоохранения и альтернативного ухода.

Источник: Замечание общего порядка № 25 (2021 г.), пп. 24-26 [28]

Ресурсы для защиты прав детей:

1. Реализация права быть услышанным при разработке собственной политики обеспечения безопасности детей в Интернете

Право быть услышанным должно занимать центральное место в практической политике обеспечения безопасности детей в Интернете. Дети и молодежь имеют собственное мнение о цифровой среде[29] и имеют право быть услышанными в вопросах, которые их касаются.[30] Для того чтобы политика обеспечения безопасности детей в Интернете отвечала их потребностям, законодатели должны прислушиваться к мнению детей и учитывать их точку зрения при разработке политики. Взгляды детей на опасности и риски, преимущества и возможности в Интернете могут отличаться от взглядов окружающих их взрослых. Поэтому эффективные консультации с участием детей[31] на протяжении всего процесса разработки, осуществления, мониторинга и оценки политики обеспечения безопасности детей в Интернете имеют решающее значение для того, чтобы обеспечить надлежащее удовлетворение их потребностей и гарантировать, что такая политика действительно будет учитывать интересы детей.[32]

28. Замечание общего порядка № 25 (2021 год) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.
29. Своими словами – права детей в цифровом мире, Фонд 5Rights, 2021 г.
30. Право быть заслушанным закреплено в статье 13 Конвенции.
31. При этом следует учитывать четыре элемента модели Ланди: пространство, голос, аудитория, влияние. См.: Модель Ланди участия детей.
32. Комиссия по цифровым перспективам.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

Модель Ланди представляет собой один из методов понимания того, «как» обеспечить участие детей по четырем основным направлениям:

Источник: Модель Ланди участия детей[33]

Необходимость учета мнения и опыта детей при разработке политики обеспечения безопасности детей в Интернете подтверждается Руководством по защите детей в Интернете Международного союза электросвязи. Учет мнений детей при рассмотрении вопроса о безопасности детей в Интернете позволяет разработать более надежную, разнообразную и инклюзивную политику.

> **Дети и молодежь хотят участвовать в обсуждении, и у них есть ценный опыт в качестве «цифровых аборигенов», которым они могут поделиться. Законодатели и специалисты-практики должны вовлекать детей и молодежь в текущие дебаты об Интернет-среде для обеспечения их прав.**
>
> Источник: Руководящие указания для директивных органов по защите ребенка в онлайновой среде, Международный союз электросвязи, 2020 г.[34]

33. Модель Ланди участия детей, Европейская комиссия, 2007 г.
34. Руководящие указания для директивных органов по защите ребенка в онлайновой среде, Международный союз электросвязи, 2020 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

2. Помощь в понимании Конвенции о правах ребенка:

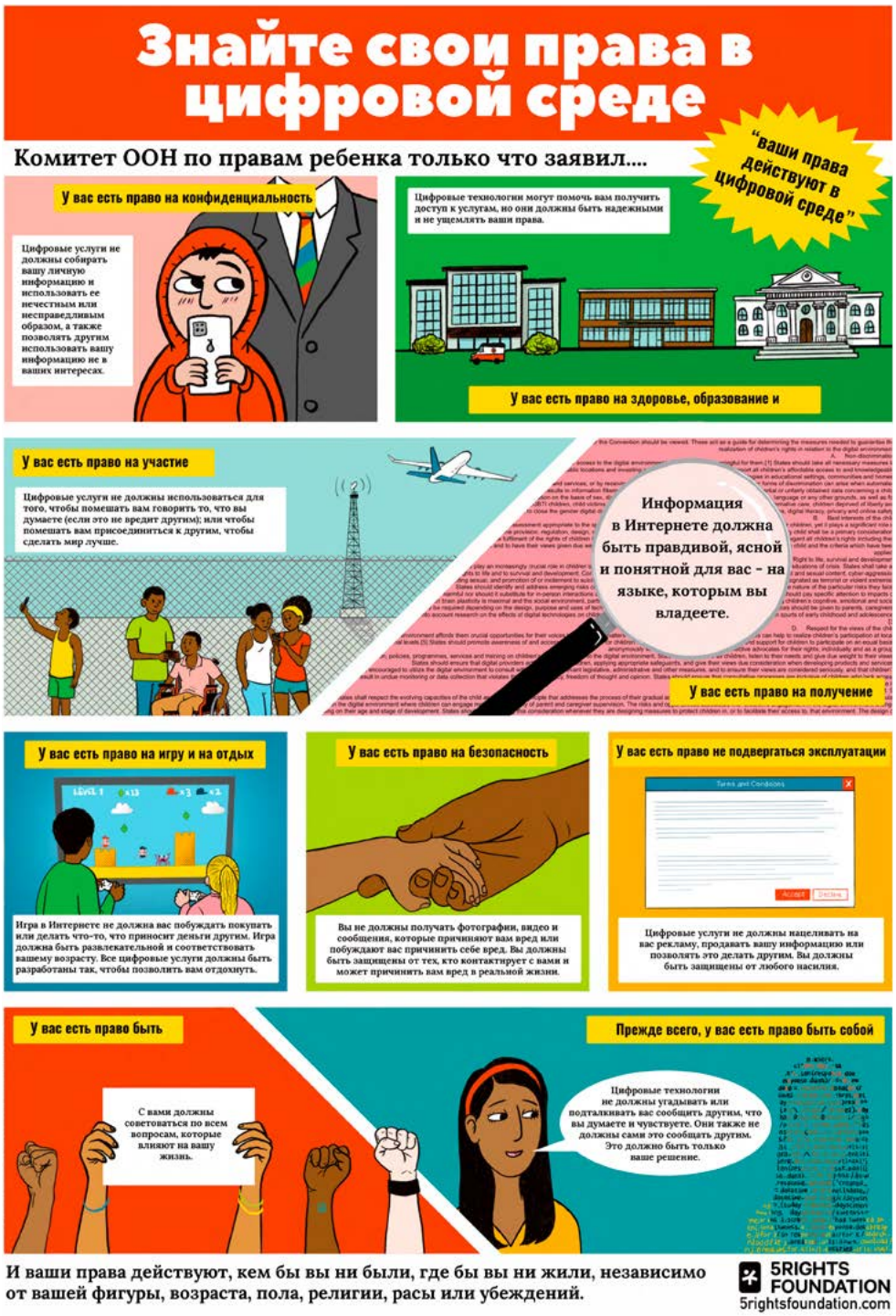
Источник: Конвенция Организации Объединенных Наций о правах ребенка (версия для детей)[35]

35. Конвенция Организации Объединенных Наций о правах ребенка (версия для детей), Save the Children, 2019 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

3. Помощь детям в понимании Замечания общего порядка № 25 (2021 г.) о правах детей в отношении цифровой среды:

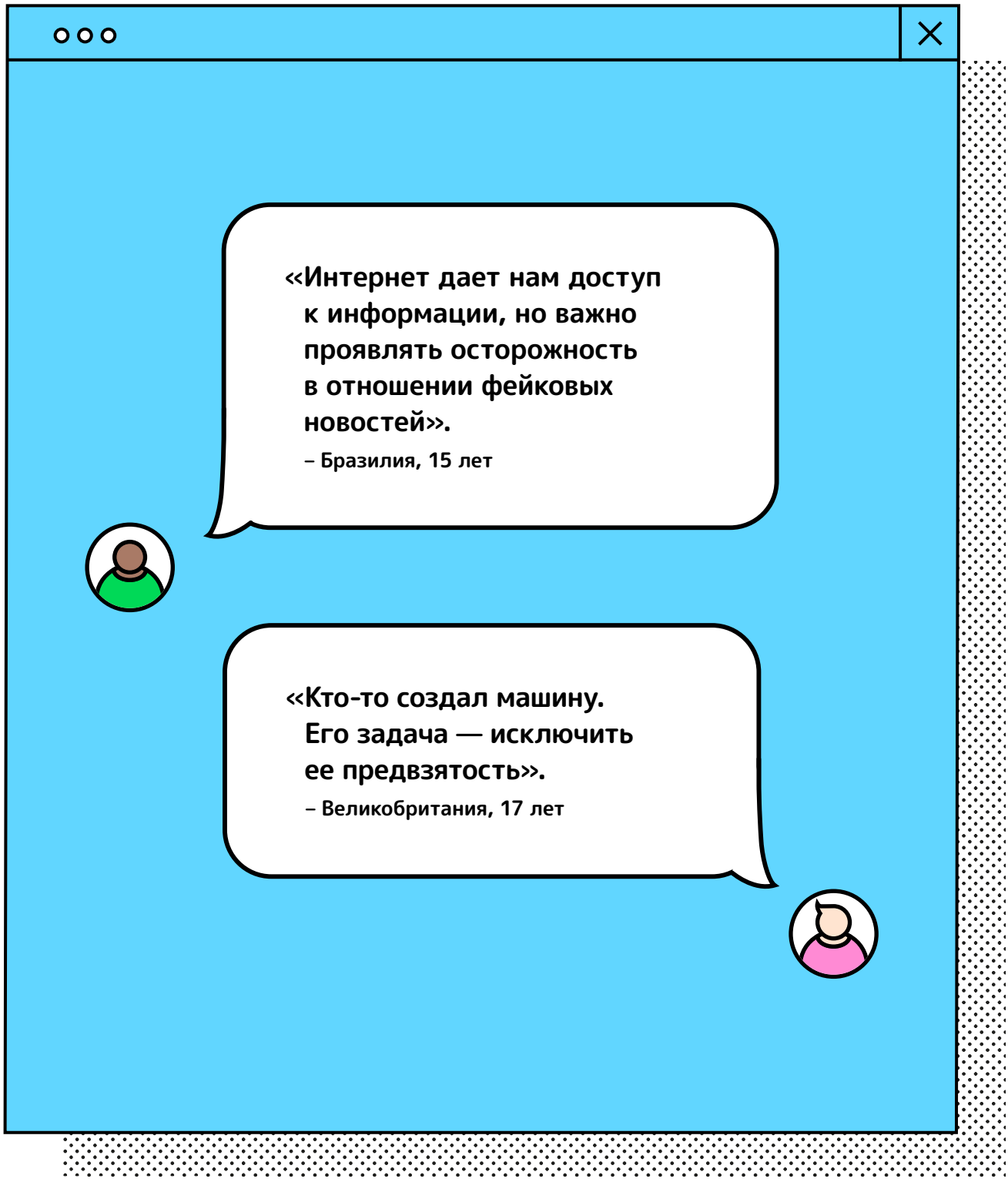


Источник: Know Your Rights! («Знай свои права!») Плакат на основе Замечания общего порядка № 25 (2021 г.)[36]

36. Знайте свои права! Плакаты на основе Замечания общего порядка № 25 (2021 год), Фонд 5Rights, 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >



СИСТЕМНАЯ ПАПКА

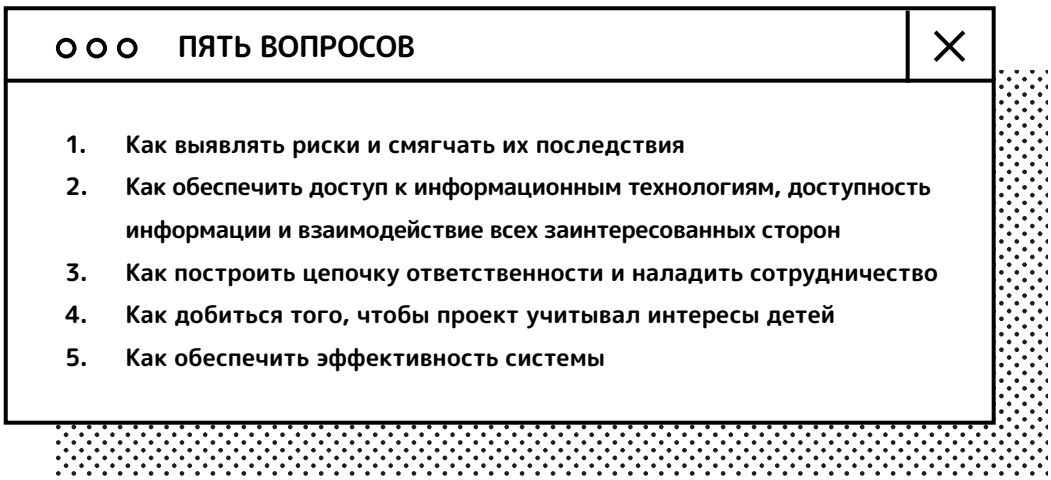
8 ДОКУМЕНТОВ | 105 МБ НА ДИСКЕ | РАЗДЕЛ 4

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

Что необходимо учитывать при разработке политики

В данном разделе рассматриваются пять межсекторальных вопросов, над которыми следует задуматься законодателям при проектировании, разработке и реализации политики обеспечения безопасности детей в Интернете.



Ответы на эти вопросы следует учитывать в десяти областях применения политики, описанных на стр. 38.

1. Как выявлять риски и смягчать их последствия:

Возможности, предоставляемые цифровой средой, играют все более важную роль в развитии детей и могут иметь огромное значение для их жизни и выживания, особенно в кризисных ситуациях. Государства-участники должны принимать все необходимые меры для защиты детей от рисков, угрожающих их праву на жизнь, выживание и развитие. Риски, связанные с содержанием, контактами, поведением и договорами, включают, в частности, содержание насильственного и сексуального характера, киберагрессию и домогательства, азартные игры, эксплуатацию и злоупотребления, в том числе сексуальную эксплуатацию и злоупотребления, а также пропаганду или подстрекательство к самоубийству или опасным для жизни действиям, в том числе со стороны преступников или вооруженных групп, признанных террористами или воинствующими экстремистами. Государства-участники должны выявлять и устранять возникающие риски, с которыми сталкиваются дети в различных контекстах, в том числе посредством изучения мнения детей о характере конкретных рисков, с которыми они сталкиваются.

Источник: Замечание общего порядка № 25 (2021 г.), п. 14[37]

Стратегии обеспечения безопасности детей в Интернете должны разрабатываться в первую очередь так, чтобы дети получали максимальную выгоду от использования цифровых технологий. Это подразумевает первостепенную ответственность за снижение рисков, минимизацию вероятности причинения вреда, устранение вреда в случае его причинения, а также анализ того, как продукция и услуги могут повлиять на конечного пользователя, если этим пользователем является (или может являться) ребенок. Ключевое значение имеет разработка продуктов и услуг, которые предполагают безопасное участие детей.

37. Замечание общего порядка № 25 (2021 год) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

В то время как некоторым детям причиняется серьезный вред, миллионы других детей в Интернете подвержены ему в той или иной форме. Например, существует широкий спектр рисков, связанных с коммерческой слежкой или эксплуатацией, распространением ложной информации или мошенничеством, преследованием или буллингом. Меньшее число детей страдает от серьезного вреда, причиняемого сексуальным насилием. Многие риски являются совокупными. Они сказываются на разных детях по-разному, и одна форма вреда может открывать возможности для других его форм.[38]

Глобальный характер цифрового мира означает, что дети сталкиваются с одинаковыми рисками независимо от своего географического положения. Однако в различных контекстах могут возникать специфические проблемы. в некоторых случаях дети могут оказаться в невыгодном положении из-за отсутствия доступа к Интернету. в других случаях может существовать связь между вредом, нанесенным в сети, и опытом ребенка в реальной жизни. Конкретные риски и вред часто накладываются друг на друга. Существует очень мало прямых взаимосвязей или точных классификаций.

Такие факторы, как гендер, возраст, семейные обстоятельства, социально-экономический статус, местоположение, опыт и доступность цифровых технологий, могут менять характер рисков и способы причинения вреда детям. Некоторые риски и вред затрагивают целые сообщества и группы детей: например, девочки чаще испытывают на себе жестокое обращение, а мальчики сталкиваются с более серьезными его проявлениями.[39] Культурные нормы, связанные с мужественностью, также усугубляют проблему недостаточного выявления случаев сексуального надругательства над детьми мужского пола и информирования о них.[40] Риски и вред могут также усиливаться платформами, разработанными для обмена шокирующим и сенсационным контентом: они могут структурировать или поощрять определенные типы поведения пользователей, поскольку это способствует прибыльному вовлечению пользователей.

Законодатели должны учитывать все риски для детей и принимать меры по их смягчению. Ключевым инструментом для выявления рисков является концепция 4C.

Классификация 4 рисков, разработанная проектом CO:RE (CO:RE 4Cs), признает, что онлайн-риски возникают, когда ребенок:

- взаимодействует с потенциально вредным **контентом** и/или подвергается его воздействию;
- устанавливает **контакт** с потенциально опасным человеком и/или становится его целью;
- становится свидетелем, участником и/или жертвой потенциально вредного **поведения**;
- является стороной потенциально опасного **договора** и/или эксплуатируется в соответствии с ним.

CO:RE	СОДЕРЖАНИЕ Ребенок как получатель	КОНТАКТ Ребенок как участник	ПОВЕДЕНИЕ Ребенок как субъект	ДОГОВОР Ребенок как потребитель
Агрессия	Насильственный, жестокий, страшный, расистский, ненавистнический и экстремистский контент	Домогательства, преследование, ненавистническое поведение, нежелательная слежка	Буллинг, ненависть или враждебные действия сверстников, например, троллинг, изоляция, шейминг	Хищение персональных данных, мошенничество, фишинг, аферы, азартные игры, шантаж, риски безопасности
Секс	Порнография (законная и незаконная), сексуализация культуры, нормы изображения тела	Сексуальные домогательства, сексуальное обольщение, создание и распространение материалов по сексуальным надругательствам над детьми	Сексуальные домогательства, сообщения сексуального содержания без согласия, сексуальное давление	Сексуальный шантаж, торговля детьми в целях сексуальной эксплуатации, передача видео сексуального насилия над детьми
Ценности	Несоответствующий возрасту пользовательский или маркетинговый контент, ложные сведения/ дезинформация	Идеологические убеждения, радикализация и вербовка экстремистов	Потенциально опасные сообщества пользователей, например, за членовредительство, против вакцинации, давление со стороны сверстников	Отбор информации, предвзятое профилирование, поляризация, убеждающий дизайн
Межсекторальные вопросы	Нарушения конфиденциальности и защиты данных, риски для физического и психического здоровья, формы дискриминации			

Источник: Содержание, контакт, поведение, контракт — обновление модели рисков 4C, CO:RE 2021 [41]

38. Построение цифрового мира, которого заслуживает молодежь, Фонд 5Rights, 2020 г.
39. Результаты инвестиционного портфеля инициативы «Безопасность в Интернете» (Safe Online) за 2020 год, Глобальное партнерство по борьбе с насилием в отношении детей, 2020 г., стр. 2.
40. Предотвращение нарушений в Кении: данные о сексуальной эксплуатации детей в Интернете и жестоком обращении с ними, Глобальное партнерство по борьбе с насилием над детьми, 2021 г., стр. 68.
41. Содержание, контакт, поведение, контракт — обновление модели рисков 4C, CO:RE 2021.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

В связи с распространением доступной широкополосной связи в развивающихся странах возникает острая необходимость в принятии мер по минимизации рисков и угроз для детей из таких стран, без ущерба для возможности пользоваться всеми преимуществами цифрового мира.

Источник: Руководящие указания для директивных органов по защите ребенка в онлайновой среде, Международный союз электросвязи, 2020 г.[42]

Государствам-участникам следует принимать во внимание меняющееся положение детей и свободу их действий в современном мире, их компетентность и понимание, которые неравномерно развиваются в различных областях навыков и деятельности, а также разнообразный характер связанных с этим рисков. Эти соображения должны быть уравновешены с важностью осуществления прав детей в поддерживаемой виртуальной среде и разнообразием их индивидуального опыта и обстоятельств. Государства-участники должны обеспечить предоставление услуг, соответствующих развивающимся способностям детей, поставщиками цифровых услуг.

Источник: Замечание общего порядка № 25 (2021 г.), п. 20[43]

2. Как обеспечить доступ к информационным технологиям, доступность информации и взаимодействие всех заинтересованных сторон:

Права каждого ребенка должны соблюдаться, защищаться и реализовываться в цифровой среде. Инновации в области цифровых технологий влияют на жизнь детей и их права широкомасштабно и взаимозависимо, даже если сами дети не имеют доступа к Интернету. Разумный доступ к цифровым технологиям может помочь детям реализовать весь спектр своих гражданских, политических, культурных, экономических и социальных прав. Однако если цифровая интеграция не будет достигнута, существующее неравенство, скорее всего, углубится, и может возникнуть новое неравенство.

Источник: Замечание общего порядка № 25 (2021 г.), п. 4[44]

Сегодня доступ к Интернету имеет решающее значение для осуществления детьми своих прав и полного раскрытия их потенциала. Политика безопасности детей в Интернете должна быть инклюзивной как по замыслу, так и на практике.[45] Это означает, что она должна опираться на достаточное количество информации, а также существующую передовую практику и нормативные рамки, особенно в ситуациях ограниченных ресурсов. Вне зависимости от того, означает ли реализация политики безопасности детей в Интернете адаптацию существующего законодательства (например, в отношении защиты детей, защиты потребителей или регулирования телекоммуникаций) к конкретным условиям или создание новых сводов законов, она должна способствовать интеграции и равенству для всех детей, независимо от того, кто они и где находятся.

Государства-участники должны поощрять технологические инновации, отвечающие требованиям детей с ограниченными возможностями, и обеспечить разработку цифровых продуктов и услуг таким образом, чтобы они были доступны для всех детей без исключения и без необходимости адаптации. Дети с ограниченными возможностями должны быть вовлечены в разработку и реализацию политики, продуктов и услуг, которые влияют на осуществление их прав в цифровой среде.

Источник: Замечание общего порядка № 25 (2021 г.), п. 91[46]

42. Руководящие указания для директивных органов по защите ребенка в онлайновой среде, Международный союз электросвязи, 2020 г.
43. Замечание общего порядка № 25 (2021 год) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.
44. Замечание общего порядка № 25 (2021 год) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.
45. Например: дети с ограниченными возможностями или дети из маргинализированных групп меньшинств, беспризорные дети, перемещенные дети и дети мигрантов, среди прочих. Данная проблема более подробно обсуждается ниже в рамках межсекторальных вопросов. Более подробную информацию о модели и контрольном списке можно найти в публикации «Одного "голоса" недостаточно: концептуализация статьи 12 Конвенции ООН о правах ребенка», Лора Ланди, 2013 г.
46. Замечание общего порядка № 25 (2021 год) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

Дети не являются однородной группой. Политика безопасности детей в Интернете должна быть доступной и инклюзивной, чтобы охватить всех детей, независимо от того, кто они и где проживают. «Цифровой разрыв» может возникнуть в тех случаях, когда некоторые дети могут легко получить доступ к цифровому пространству, а у других такой возможности фактически нет. Нормативные рамки должны соответствовать возрасту и охватывать всех детей независимо от пола, расы, религии, национальности, этнической принадлежности, инвалидности или любых других характеристик. Формулировки должны быть доступными и инклюзивными, и, при необходимости, материалы должны быть доступны на разных языках. Материалы по безопасности детей в Интернете должны разрабатываться на основе консультаций с детьми и родителями/опекунами: как минимум, они должны соответствовать возрасту, быть нейтральными с гендерной точки зрения и легкодоступными для детей разных возрастов и их родителей/опекунов. в случае ограничений, связанных с грамотностью, более эффективными часто являются визуальные материалы. Единообразие терминологии на различных платформах обеспечивает большую доступность информации о безопасности детей в Интернете для детей, их семей и опекунов.[47]

Законодатели должны содействовать доступу детей в Интернет и вовлекать их в процесс создания безопасной цифровой среды.

> **Взрослые и дети подвергаются различным рискам и опасностям в Интернете. Тем не менее дети являются гораздо более уязвимой группой населения. Некоторые дети также находятся в более уязвимом положении, чем другие группы детей, например дети с ограниченными возможностями или постоянно переезжающие дети. Законодатели должны гарантировать всем детям возможность развиваться и получать образование в безопасной цифровой среде. Идея о том, что дети уязвимы и должны быть защищены от всех форм эксплуатации, изложена в Конвенции ООН о правах ребенка.**
>
> Источник: Руководящие указания для директивных органов по защите ребенка в онлайновой среде, Международный союз электросвязи, 2020 г.[48]

3. Как построить цепочку ответственности:

> **Чтобы охватить межсекторальные последствия влияния цифровой среды на права детей, государства-участники должны определить правительственный орган, уполномоченный координировать политику, руководящие принципы и программы, касающиеся прав детей, между центральными правительственными департаментами и различными уровнями правительства. Такой национальный координационный механизм должен взаимодействовать со школами и сектором информационно-коммуникационных технологий, а также сотрудничать с предприятиями, гражданским обществом, научными кругами и организациями для реализации прав детей в отношении цифровой среды на межсекторальном, национальном, региональном и местном уровнях. Он должен опираться на технический и другой соответствующий опыт внутри правительства его и за пределами, по мере необходимости, и проходить независимую оценку эффективности выполнения своих обязательств.**
>
> Источник: Замечание общего порядка № 25 (2021 г.), п. 27[49]

Ответственность за обеспечение безопасности детей в Интернете лежит на многих людях, специалистах и организациях, включая правительство, правоохранительные органы, бизнес, педагогов, службы психологической и социальной поддержки, семьи и самих детей. Некоторые звенья в этой цепочке несут большую ответственность, чем другие.[50] Например, разработчики сервиса, доступ к которому может быть предоставлен детям или который может повлиять на них, должны учитывать, представляет ли какая-либо из функций риск для детей. Это необходимо сделать до того, как привлекать детей к использованию такого сервиса. Это часто называют «встроенной безопасностью» или «проектами, учитывающими интересы детей». Встроенная безопасность должна быть нормой.

47. См. введение о важности формулировок и определений и раздел «Глоссарий».
48. Руководящие указания для директивных органов по защите ребенка в онлайновой среде, Международный союз электросвязи, 2020 г.
49. Замечание общего порядка № 25 (2021 год) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.
50. См., например, Руководящие принципы предпринимательской деятельности в аспекте прав человека, ООН.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

Цепочка ответственности заинтересованных сторон

Ответственность за безопасность детей в Интернете включает в себя как предотвращение вреда, так и принятие мер по его смягчению и устранению. Инструменты подачи жалоб и сообщений о нарушениях должны быть доступными и четко обозначенными, чтобы дети, опекуны и специалисты, которые в них нуждаются, могли легко находить и использовать их. в рамках цифровых коммерческих систем следует создать механизмы, позволяющие отслеживать и оценивать сообщения о нарушениях. Это позволит оперативно выявлять и решать проблемы.

Законы и нормативные акты должны устанавливать четкие рамки для предотвращения проблем, а также несения ответственности и возмещения вреда в случае их возникновения. Это включает сбор данных о сообщениях и жалобах, чтобы они контролировались и анализировались в целях совершенствования системы. Дети и родители/опекуны не должны нести ответственности за предотвращение или устранение рисков и вреда, которые они плохо понимают или не могут контролировать. Согласие не может использоваться для освобождения государственных или частных организаций от их ответственности за безопасность детей в Интернете. Включение вопросов безопасности детей в Интернете в существующие механизмы обеспечения безопасности продуктов[51], защиты детей[52], прав детей[53] и прав потребителей[54] поможет устранить пробелы в цепочке ответственности и дублирования ресурсов, ролей и обязанностей. Не должно существовать никаких правовых лазеек, снижающих эффективность защиты детей в Интернете.

Крайне важно, чтобы безопасность детей в Интернете была интегрирована во все соответствующие области политики, начиная с национальных планов развития широкополосной связи и заканчивая учебными программами. Интеграция должна быть выполнена таким образом, чтобы она была прозрачной, подотчетной и реализуемой. Создание разрозненных систем может привести к возникновению конфликтов в области регулирования и фрагментации процесса разработки и осуществления политики.

Законодатели должны осознать всю сложность ответственности за безопасность детей в Интернете и обеспечить наличие механизмов сотрудничества и поддержки для всех участников цепочки, чтобы они могли играть свою роль в защите детей. Чрезвычайно важное значение имеет также четкое понимание ролей, обязанностей и ведущих участников деятельности в конкретных областях.

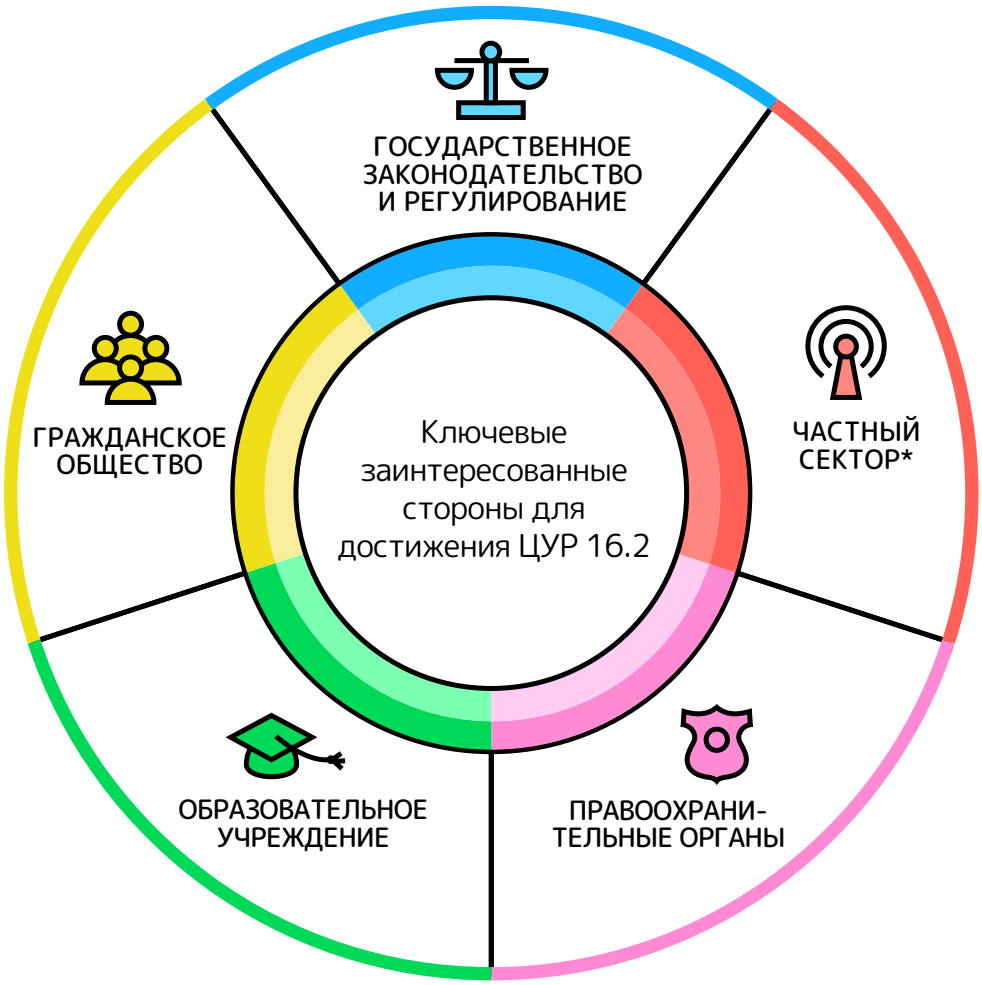
> **Защита детей и молодежи является общей обязанностью, и все заинтересованные стороны должны обеспечить устойчивое будущее для всех. Чтобы это произошло, законодатели, представители отрасли, родители, опекуны, педагоги и другие заинтересованные стороны должны предоставить детям и подросткам возможность реализовать свой потенциал как в Интернете, так и за его пределами.**
>
> Источник: Руководящие указания для директивных органов по защите ребенка в онлайновой среде, Международный союз электросвязи, 2020 г.[55]

> **Надлежащее управление должно объединять тех, кто несет ответственность за защиту детей от сексуальной эксплуатации в Интернете, и осуществляться многосторонним, межотраслевым национальным органом или органами. Не существует единой модели, которую должен принять такой многосторонний орган: он может отвечать как за общее управление и надзор за возможностями и способностью страны по предотвращению сексуальной эксплуатации детей и жестокого обращения с ними (CSEA) в Интернете и оперативному реагированию, так и просто выступать в качестве органа, координирующего работу представителей правительства, отрасли и гражданского общества.**
>
> Источник: Модель национального реагирования Глобального альянса WeProtect 2016 г.[56]

51. Стандарты и риски для конкретных продуктов, Европейская комиссия, 2014 г.
52. Центр защиты детей, Европейская комиссия, 2021 г.
53. Стратегия по правам ребенка, Совет Европы, 2021 г.
54. Директива по правам потребителей, Европейская комиссия, 2014 г.
55. Руководящие указания для директивных органов по защите ребенка в онлайновой среде, Международный союз электросвязи, 2020 г.
56. Предотвращение сексуальной эксплуатации детей и жестокого обращение с ними (CSEA): Модель национального реагирования, Глобальный альянс WeProtect, 2 016 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

Эти обязанности также отражены в других обязательствах, включая Цели устойчивого развития, где они закреплены в цели 16.2: «положить конец жестокому обращению, эксплуатации, торговле и всем формам насилия и пыткам в отношении детей».



*Включает операторов, интернет-провайдеров, поставщиков контента, социальные сети и платформы обмена сообщениями

Источник: Безопасность детей в Интернете: минимизация риска насилия, жестокого обращения и эксплуатации онлайн, Комиссия по широкополосной связи, 2019 год[57]

57. Безопасность детей в Интернете: минимизация риска насилия, жестокого обращения и эксплуатации онлайн, Комиссия по широкополосной связи, 2019 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

4. Как добиться того, чтобы проект учитывал интересы детей:

> **Государства-участники должны регулировать защиту от известного вреда и активно анализировать новые исследования и факты в отрасли общественного здравоохранения в целях предотвращения распространения ложных сведений, а также материалов и услуг, которые могут причинить вред психическому или физическому здоровью детей. Также могут потребоваться меры по предотвращению нездорового участия в цифровых играх или социальных сетях, такие как регулирование против цифрового дизайна, который подрывает развитие и права детей.**
>
> Источник: Замечание общего порядка № 25 (2021 г.), п. 96[58]

Безопасность детей в Интернете должна учитываться при проектировании и разработке технологий. Проекты, учитывающие интересы детей, с самого начала закладывают безопасность детей в Интернете в услуги и продукты. в частности, речь идет о включении безопасности детей в Интернете в нормативные требования к проектированию и лицензированию новых технологий[59]. Проекты, учитывающие интересы детей, также можно назвать проектами со встроенными безопасностью, правами, конфиденциальностью и этикой.

Применение принципа предотвращения[60] к технологиям, которые могут повлиять на детей и молодежь, гарантирует учет проблем безопасности детей в Интернете на самой ранней стадии разработки. Всемирная комиссия ЮНЕСКО по этике научных знаний и технологий (КОМЕСТ) предложила «рабочее определение» принципа предотвращения:

> **«Когда деятельность человека приводит к морально неприемлемому ущербу, который является научно обоснованным, но неопределенным, необходимо принять меры для предотвращения или снижения такого ущерба.**
>
> Под морально неприемлемым ущербом понимается вред, причиненный человеку или окружающей среде, который:
>
> - **представляет угрозу жизни или здоровью человека;**
> - **является серьезным и практически необратимым;**
> - **является несправедливым по отношению к нынешнему или будущим поколениям;**
> - **наносится без надлежащего учета прав пострадавших».[61]

Принцип предотвращения должен лежать в основе концепции встроенных безопасности и конфиденциальности для обеспечения безопасности детей в Интернете и включения их прав в технологию на этапе проектирования. Учет интересов детей должен быть не только этической концепцией, но и юридическим требованием.[62] Он также должен стать одним из критериев финансирования научно-исследовательской работы, которая может затрагивать права детей в Интернете.

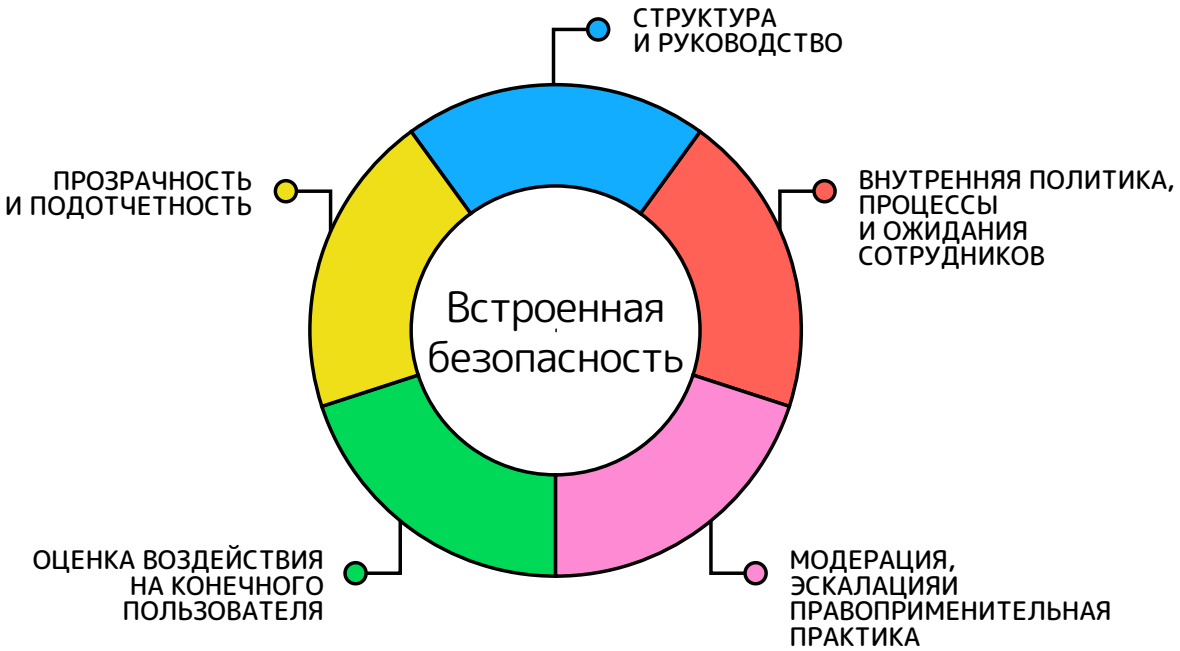
Технологии и искусственный интеллект (ИИ) способны повысить безопасность детей в Интернете и защитить их права. Одним из важных аспектов политики в этой области является содействие разработке технических средств для реализации прав детей и повышения их безопасности в Интернете. Более широкое применение ИИ или других технологий, предназначенных для защиты детей, должно оцениваться в свете всех прав ребенка[63] с тем, чтобы не подрывать некоторые из них, такие как право на неприкосновенность частной жизни и свободу от дискриминации.

58. Замечание общего порядка № 25 (2021 год) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.
59. Добровольные принципы противодействия сексуальной эксплуатации детей и жестокому обращению с ними в Интернете, GOV.UK, 2021 г.
60. См. Сообщение Комиссии о принципе предотвращения EUR-Lex, 2000 г.; Принцип предотвращения: определения, применение и управление, Европейский парламент, 2015 г.
61. Принцип предотвращения, Всемирная комиссия по этике научных знаний и технологий, 2005 г.
62. См. например, статью 25 Общего регламента о защите данных, Европейский союз, 2018 г.
63. См. например, Замечание общего порядка № 25 (2021 год) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

Дети являются чрезвычайно неоднородной группой, и при разработке, осуществлении и мониторинге эффективности политики в этой области следует учитывать весь спектр характеристик и условий жизни детей. Эффективные действия по обеспечению безопасности детей в Интернете должны быть направлены на устранение существующих противоречий. Например, в дебатах по шифрованию аргументы сторонников борьбы с сексуальной эксплуатацией детей и жестоким обращением с ними (CSEA) могут противоречить аргументам, связанным с конфиденциальностью и защитой данных. Такие конфликты должны разрешаться в той мере, в какой это возможно на практике с тем, чтобы избежать многолетних дискуссий, в то время как дети подвергаются риску или страдают. в таких случаях интересы ребенка должны иметь первостепенное значение.[64]

Существует несколько механизмов и процессов, которые поддерживают проекты, учитывающие интересы ребенка, при разработке политики, включая принцип предотвращения, оценку воздействия на права детей[65] и консультации с детьми.[66] Кроме того, Ассоциация стандартов Института инженеров электротехники и электроники (IEEE-SA) разработали стандарт, предусматривающий практические шаги, которым компании могут следовать для разработки цифровых продуктов и услуг с учетом возраста пользователей,[67] а Комиссия по цифровым перспективам определила, как право детей на свободную игру может быть поддержано в цифровом мире путем улучшения дизайна продуктов и услуг. Законодатели должны всегда стремиться к тому, чтобы разработчики сводили к минимуму риск, прежде чем их продукты и услуги станут доступными для детей. Принципы встроенных безопасности и прав носят системный характер и поэтому направлены на защиту миллионов детей с самого начала, а не после того, как что-то случится.



Источник: Инициатива встроенной безопасности,[68] Инструменты и принципы самооценки,[69] eSafety

64. Конвенция о правах ребенка, Управление Верховного комиссара Организации Объединенных Наций по правам человека, 1989 г. (См., в частности, раздел 1 статьи 3 о правах детей).
65. Оценка воздействия на права ребенка, Комиссия по цифровым перспективам, 2021 г.
66. Оценка воздействия на права ребенка, Комиссия по цифровым перспективам, 2021 г.
67. Стандарт для рамочных цифровых услуг с учетом возраста IEEE 2089-21, IEEE SA, 2021 г.
68. Принципы встроенной безопасности, Комиссар по электронной безопасности, 2021 г.
69. Принципы встроенной безопасности, Комиссар по электронной безопасности, 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

5. Как обеспечить эффективность системы:

Государства-участники должны мобилизовать, выделять и использовать государственные ресурсы для реализации законодательства, политики и программ, направленных на полную реализацию прав детей в цифровой среде и на улучшение цифровой инклюзивности для решения проблемы растущего влияния цифровой среды на жизнь детей и для содействия равенству в области доступа к услугам и их доступности, а также для обеспечения возможности подключения к сети.

Государства-участники должны обеспечить, чтобы мандаты национальных правозащитных учреждений и других соответствующих независимых институтов охватывали права детей в цифровой среде, и чтобы они могли получать, расследовать и рассматривать жалобы от детей и их представителей. Там, где существуют независимые надзорные органы для мониторинга деятельности в отношении цифровой среды, национальные правозащитные учреждения должны тесно сотрудничать с такими органами в целях эффективного выполнения их мандата в отношении прав детей.

Источник: Замечание общего порядка № 25 (2021 г.), пп. 28 и 31[70]

Безопасность детей в Интернете и защита их прав в цифровой среде могут быть по-настоящему эффективными только при наличии практических политических действий, достаточного финансирования и правоохранительных мероприятий.

Безопасность детей в Интернете имеет отношение к широкому кругу областей политики, включая информационно-коммуникационные технологии (ИКТ), образование, уголовное правосудие, здравоохранение, регулирование отрасли, социальную и семейную поддержку, предпринимательство, права человека и равенство, международное развитие и многие другие. Таким образом, сотрудничество между различными министерствами и ведомствами, работающими в стратегических областях, имеет важнейшее значение для эффективной деятельности по обеспечению безопасности детей в Интернете. Чтобы обеспечить ресурсы для осуществления политики как в рамках различных департаментов, так и между ними, необходимо финансирование. Политика с недостаточным финансированием или партнерство без возможностей, то есть то, что существует только на бумаге, не приведет к эффективной защите детей в Интернете.

Понимание принципов эффективности означает пересмотр влияния политики на безопасность детей в Интернете. Мониторинг, оценка и сбор данных являются ключевыми факторами для разработки качественной политики. Одним из лучших способов максимального повышения эффективности является извлечение уроков и обмен опытом в области разработки эффективной трансграничной политики. Проверка эффективности политики обеспечения безопасности детей в Интернете требует проведения консультаций не только с основными заинтересованными сторонами, но и с детьми, чтобы понять, каким образом такая политика влияет на них или может повлиять в будущем.[71] Это непрерывный процесс.

Политика должна быть основана на данных и фактах. Как соответствующие органы, так и частные компании должны собирать данные и обмениваться ими в целях лучшего понимания проблем в области безопасности детей в Интернете в соответствии с законами и принципами защиты данных. Безопасность детей в Интернете является относительно новой областью политики, поэтому в тех случаях, когда доказательства отсутствуют или оспариваются, законодатели должны применять принцип предотвращения или использовать эффективные подходы, работающие в других условиях: например, обращаться к областям здравоохранения или безопасности либо к таким концепциям, как «Семь стратегий по искоренению насилия в отношении детей» (INSPIRE).[72]

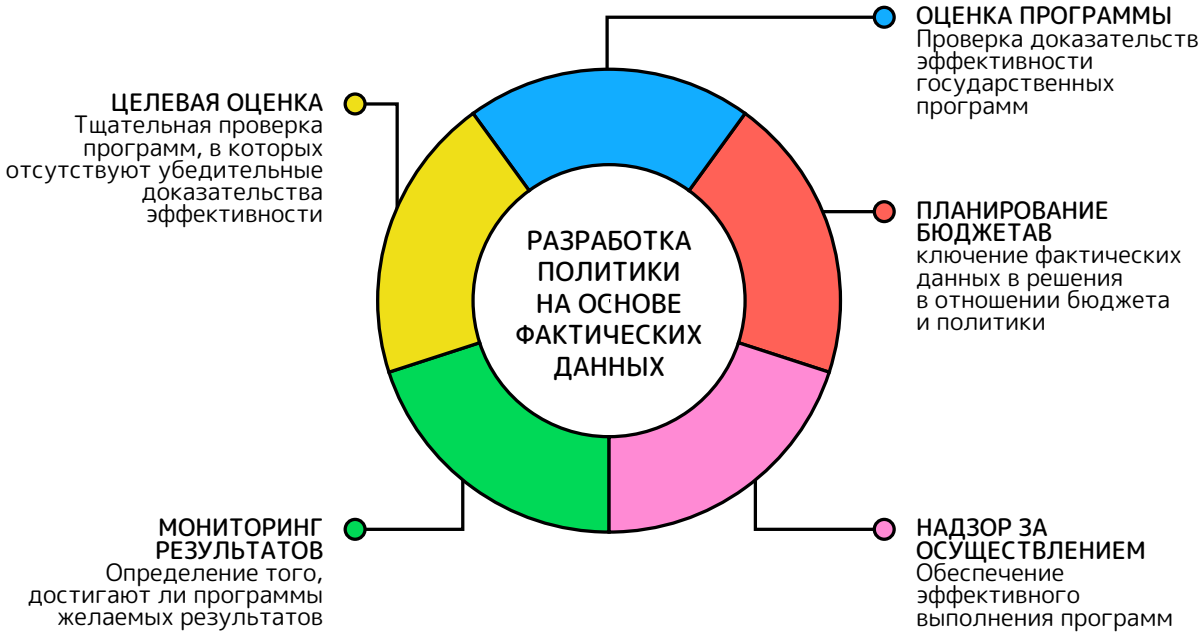
Безопасность детей в Интернете не является обособленной проблемой. Эффективность политики в этой области будет зависеть от общей продуктивности ключевых учреждений и их способности сотрудничать в целях обеспечения надежной защиты. Обеспечение эффективной подотчетности в области безопасности детей в Интернете в целом и предотвращение сексуальной эксплуатации детей и жестокого обращения с ними (CSEA) в частности основывается на сильной национальной системе правосудия. Руководство по этому вопросу содержится в Модели национального реагирования (MNR). Эффективные подходы к обеспечению безопасности детей в Интернете также зависят от наличия достаточных ресурсов для соответствующих учреждений, в том числе в таких областях, как психологическая и социальная поддержка, а также регулирование ИКТ и смежных сфер. Эффективная защита прав ребенка с помощью политики обеспечения безопасности детей в Интернете зависит от действенного законодательства в области прав человека, а также конкретных законов и регулирования со стороны органов надзора в целях, гарантирующих права детей как в цифровой среде, так и в реальной жизни.

70. Замечание общего порядка № 25 (2021 год) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.
71. Комиссия по цифровым перспективам, Фонд 5Rights, 2021 г.
72. Руководство по показателям и матрица результатов программы INSPIRE, Всемирная организация здравоохранения, 2018 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

Законодатели должны обеспечить наличие возможностей вовлеченных организаций, ресурсов и механизмов подотчетности для поддержки политики обеспечения безопасности детей в Интернете. В случае возникновения конфликтов первостепенное значение должны иметь интересы ребенка. Без этого даже самая качественная политика будет неэффективной.

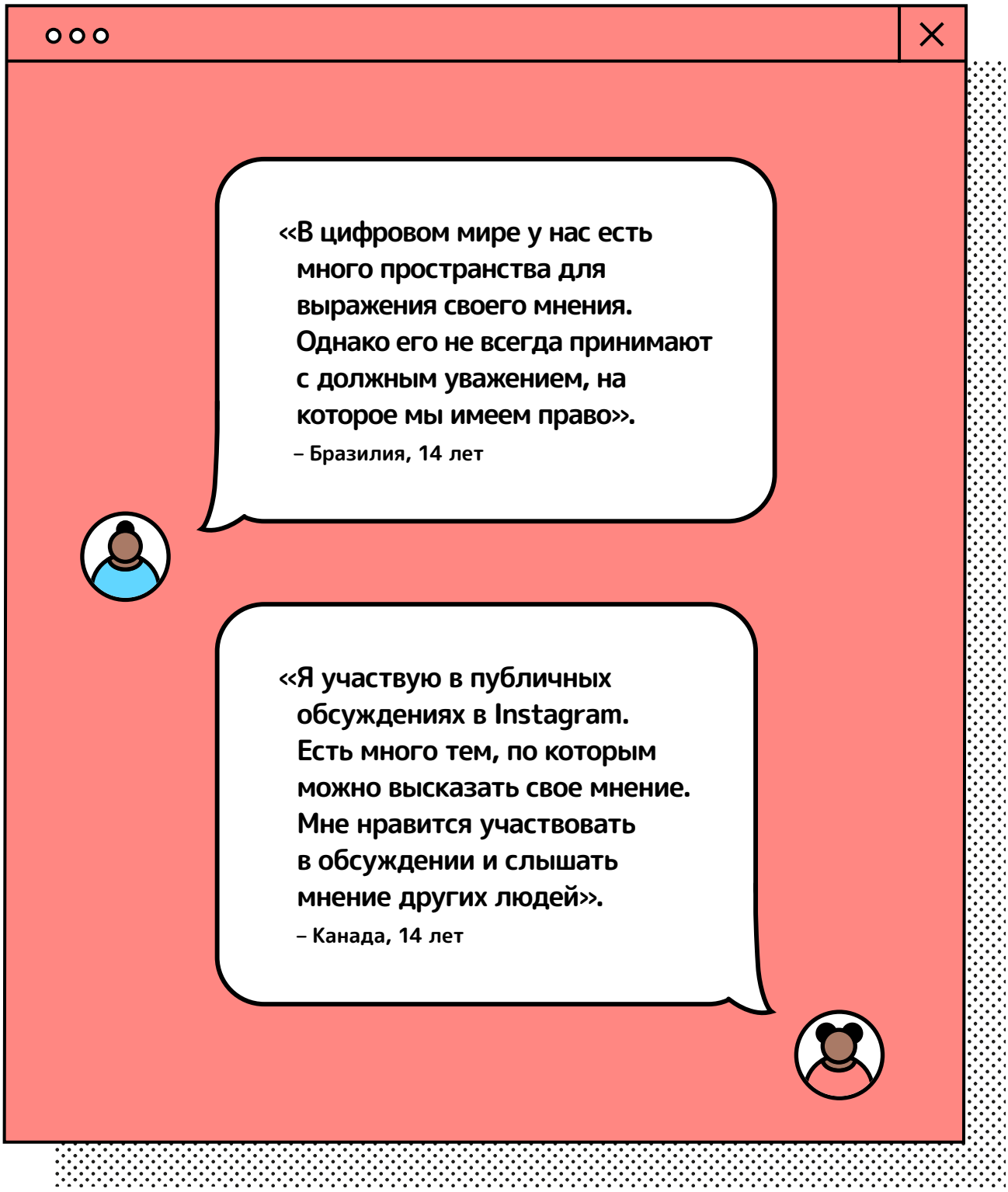


Источник: Разработка политики на основе фактических данных, Pew Charitable Trusts/MacArthur Foundation[73]

73. Разработка политики на основе фактических данных, Фонд МакАртура, 2014 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >



СИСТЕМНАЯ ПАПКА

8 ДОКУМЕНТОВ | 105 МБ НА ДИСКЕ | РАЗДЕЛ 5

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

Десять областей применения политики

В данном разделе представлены типовые политики, в которых описаны практические действия, необходимые для осуществления эффективной политики обеспечения безопасности детей в Интернете, а также инструменты для законодателей по разработке и внедрению эффективных механизмов, соответствующих национальному контексту.

ТИПОВЫЕ ПОЛИТИКИ

1. Возможности вовлеченных организаций
2. Нормативно-правовое регулирование
3. Персональные данные, идентичность и самостоятельность
4. Системы реагирования и поддержки
5. Корпоративная ответственность
6. Обучение
7. Образовательные программы
8. Связи с общественностью и формирование коллективной сознательности
9. Научно-исследовательская работа
10. Международное сотрудничество

При осуществлении этих конкретных мер необходимо учитывать четыре руководящих принципа в области прав детей, которые изложены в главе 3:

ПРИНЦИПЫ

- Право на свободу от дискриминации
- Интересыребенка
- Право на жизнь, выживание и развитие
- Право быть услышанным

И пять других межсекторальных вопросов, изложенных в разделе A:

ПЯТЬ ВОПРОСОВ

- Риск и вред
- Доступность и инклюзивность
- Цепочка ответственности
- Учет интересов детей
- Эффективность

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

1 Возможности вовлеченных организаций

> **Государства-участники должны принять законодательные и административные меры для защиты детей от насилия в цифровой среде, включая регулярный пересмотр, обновление и обеспечение соблюдения надежной законодательной, нормативной и институциональной базы, которая защищает детей от существующих и вновь возникающих рисков всех форм насилия в цифровой среде.**
>
> Источник: Замечание общего порядка № 25 (2021 г.), п. 82[74]

Цель

Определить ведущее министерство или ведомство для создания Национального руководящего комитета по безопасности детей в Интернете и группы экспертов заинтересованных сторон для охвата всех областей политики безопасности детей в Интернете. Обеспечить наличие адекватные ресурсы, руководство и возможности вовлеченных организаций для реализации эффективности деятельности и сотрудничества.

Текст типовой политики

Для обеспечения целостного подхода к безопасности детей в Интернете необходимо предпринять следующие шаги.

1a. Подтвердить государственную поддержку вопросам безопасности детей в Интернете на самом высоком уровне
Национальные лидеры, включая премьер-министра или президента, должны взять на себя обязательство обеспечивать безопасность детей в Интернете как на национальном, так и на международном уровнях.

1b. Назначить министерство или ведомство, которое возьмет на себя ведущую роль при разработке национальной политики безопасности детей в Интернете
Во всем мире целый ряд различных учреждений и министерств играют ведущую роль в разработке политики безопасности детей в Интернете. Выбор такого учреждения или министерства может повлиять на то, как будет развиваться политика и каким аспектам будет уделено наибольшее внимание. Безопасность детей в Интернете, вероятно, будет вопросом, рассматриваемым в нескольких министерствах, однако за повестку дня должно отвечать одно ведущее ведомство. в некоторых странах такая политика осуществляется под руководством министерства по вопросам ИКТ, в других — министерства по делам детей и семей или юстиции. Существующие группы, отвечающие за вопросы насилия в отношении детей (VAC) или кибербезопасности, могут быть расширены с тем, чтобы включить в них необходимый экспертный потенциал для предотвращения изолированной работы. *Ведущее ведомство может быть выбрано с учетом его авторитета, опыта, ресурсов, потенциала или энтузиазма, однако важным условием является его сотрудничество с другими учреждениями.* Независимо от того, какое министерство возьмет на себя ведущую роль, оно должно придерживаться целостного подхода, отражающего все потребности, связанные с безопасностью детей в Интернете.

1c. Опубликовать руководство по терминологии и языку
Назначенное ведущее министерство должно опубликовать полный перечень терминов и формулировок, используемых в международной передовой практике.[75] ▶

74. Замечание общего порядка № 25 (2021 г.) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.
75. См., например, Универсальная терминология: Терминологическое руководство по защите детей от сексуальной эксплуатации и сексуального насилия, ECPAT International, 2016 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

1d. Создать Национальный руководящий комитет по безопасности детей в Интернете
Национальный руководящий комитет по безопасности детей в Интернете должен отвечать за осуществление и разработку политики, а также выполнять функции координационного центра по вопросам национального и регионального сотрудничества. в его задачи будет входить использование Набора программных средств для обеспечения безопасности детей в Интернете и разработка плана действий по его реализации. Комитет будет заниматься широким кругом вопросов, охватывающих различные области политики, включая, в частности, образование, здравоохранение, правосудие, защиту потребителей, защиту данных, правоохранительную деятельность, информационно-коммуникационные технологии, а также услуги для семьи и детей, и контролировать внедрение и поддержку стандартов. Комитет должен официально сотрудничать со всеми учреждениями, ответственными за безопасность или кибербезопасность детей, и регулярно отчитываться перед ведущим министерством.

1e. Выявить заинтересованные стороны в области безопасности детей в Интернете
Правоприменительное сообщество, предприятия, третий сектор, организации по защите прав детей, образовательные учреждения, родители/опекуны и научные круги имеют полезные знания и собственную заинтересованность в области безопасности детей в Интернете. в некоторых условиях создание группы заинтересованных сторон может быть полезным для поддержки Комитета в его деятельности и обоснования плана действий в реальных сценариях. в других контекстах более эффективными могут быть неформальные дискуссии или получение необходимой информации из открытой сети заинтересованных сторон. в любом случае Национальный руководящий комитет по безопасности детей в Интернете должен стремиться к взаимодействию с ключевыми заинтересованными сторонами, которые могут поддержать его деятельность. Следует поощрять межведомственное сотрудничество. Целью вовлечения заинтересованных сторон является сосредоточение внимания на осуществлении, а не на разработке политики.

1f. Определить роли и обязанности заинтересованных сторон
Должна существовать совместная нормативно-правовая база, определяющая роли и обязанности всех организаций, разрабатывающих цифровую инфраструктуру, сети и сервисы, а также управляющих ими, и обязанности государственных ведомств. Следует установить минимальные стандарты для всех участников цепочки создания стоимости, включая тех, кто отвечает за инфраструктуру, аппаратные средства и цифровые продукты и услуги, а также тех, кто управляет ими или использует их при взаимодействии с детьми. Эти стандарты должны быть сосредоточены на безопасности детей и полной реализации их прав в цифровом мире. Следует обеспечить участие гражданского общества и консультирование детей в группах заинтересованных сторон.

1g. Установить показатели эффективности и систему оценки
Для каждого аспекта плана реализации нужно определить соответствующий ответственный орган (лицо, учреждение, ведомство) и людские и финансовые ресурсы для успешного выполнения поставленной задачи. Один и тот же орган может отвечать сразу за несколько областей политики или только за одну из них. Чтобы Руководящий комитет мог осуществлять надзор и отслеживать прогресс, следует внедрить ключевые показатели эффективности (KPI), механизмы оценки и четкие структуры отчетности. в связи с быстрым развитием цифровой среды KPI необходимо постоянно пересматривать.

1h. Обеспечить интеграцию вопросов безопасности детей в Интернете во все области государственной политики
Любые профильные национальные планы, такие как Национальный план развития широкополосной связи или рамочная программа обеспечения компьютерной грамотности, должны включать политику обеспечения безопасности детей в Интернете как часть стратегии внедрения. Планы, которые осуществляются в течение нескольких лет, должны пересматриваться на ключевых этапах.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

1 Возможности вовлеченных организаций

План мероприятий для достижения цели

A **Подтвердить государственную поддержку вопросам безопасности детей в Интернете на самом высоком уровне**

Национальные лидеры, включая премьер-министра, президента или министров, должны взять на себя обязательство обеспечивать безопасность детей в Интернете как на национальном, так и на международном уровнях.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, составьте план, полностью подтвержденный широкой группой сторонников, и донесите его до национальных лидеров. в вашем плане следует:

1. Предоставить обоснование с соответствующими доказательствами и данными; если данные по вашей стране отсутствуют, используйте международные данные.
2. Определить ключевых лиц, принимающих решения, и направьте на них правозащитные усилия, основанные на конкретных доказательствах, чтобы добиться их понимания и принятия на себя обязательств.
3. Найти сторонников и экспертов (внутренних, местных и международных) и заручиться их поддержкой.
4. Изучить национальные меры и политики, направленные на обеспечение безопасности детей в Интернете и борьбу с другими формами насилия в отношении детей (VAC), женщин и девочек (VAWG), а также кибербезопасности.
5. На основе вышеизложенного договориться (по согласованию с ключевыми заинтересованными сторонами) о том, как реализовать целостную политику безопасности детей в Интернете, включающую существующие программы и опирающуюся на них.
6. Выяснить существующие обязанности и обязательства в рамках имеющихся нормативных документов и других действующих национальных планов действий и межсекторальных комитетов (включая VAC, VAWG, кибербезопасность).
7. Составить план действий после консультации с ключевыми заинтересованными сторонами: с указанием затрат, сроков и ведущего ведомства, а также конкретного лица или организации, ответственного(-ой) за каждое мероприятие.
8. Довести план мероприятий до сведения лиц, принимающих решения, заручившись полной поддержкой, чтобы получить их согласие и подпись.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

1 Возможности вовлеченных организаций

B **Назначить министерство или ведомство, которое возьмет на себя ведущую роль при разработке национальной политики безопасности детей в Интернете**

Во всем мире политикой обеспечения безопасности детей в Интернете занимаются различные ведомства и министерства, и выбор ведомства или министерства может повлиять на то, как будет развиваться политика обеспечения безопасности детей в Интернете, и каким ее аспектам будет уделено наибольшее внимание. Безопасность детей в Интернете, вероятно, будет вопросом, рассматриваемым в нескольких министерствах, однако за повестку дня должно отвечать одно ведущее ведомство. в одних странах такая политика осуществляется под руководством министерства по вопросам ИКТ, в других — министерства по делам детей и семей или министерства юстиции. Ведущее ведомство может быть выбрано с учетом его авторитета, опыта, ресурсов, потенциала или энтузиазма, однако важным условием является его сотрудничество с другими учреждениями. Независимо от того, какое министерство возьмет на себя ведущую роль, оно должно придерживаться целостного подхода, отражающего все потребности, связанные с безопасностью детей в Интернете.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, используйте SWOT-анализ. См. Средства поддержки 1 (стр. 47) для выбора ведущего министерства или ведомства.

C **Опубликовать руководство по терминологии и языку**

Назначенное ведущее министерство должно издать полный перечень терминов и формулировок, используемых в международной передовой практике.[76]

Если эти шаги выполнены, убедитесь, что он соответствует глоссарию и определениям (на стр. 178), чтобы обеспечить эффективный перевод.

Если нет, используйте глоссарий и определения (стр. 178) для обеспечения эффективного перевода.

76. См., например, Универсальная терминология: Терминологическое руководство по защите детей от сексуальной эксплуатации и сексуального насилия, ECPAT International, 2016 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

1 Возможности вовлеченных организаций

D **Национальный руководящий комитет по безопасности детей в Интернете**

Национальный руководящий комитет по безопасности детей в Интернете должен отвечать за осуществление и разработку политики, а также выполнять функции координационного центра по вопросам национального и регионального сотрудничества. Он разработает стратегию по внедрению Набора программных средств для обеспечения безопасности детей в Интернете. Комитет будет заниматься широким кругом вопросов, охватывающих различные области политики, включая, в частности, образование, здравоохранение, правосудие, защиту потребителей, защиту данных, правоохранительную деятельность, информационно-коммуникационные технологии, а также услуги для семьи и детей, и контролировать внедрение и поддержку стандартов. Комитет должен быть подотчетен ведущему министерству.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Подумать, какие министерства и правительственные организации могут внести свой вклад в эффективную реализацию политики обеспечения безопасности детей в Интернете, и организовать регулярные консультации.
2. Подумать, какое региональное или местное представительство может быть заинтересовано в обеспечении безопасности детей в Интернете.
3. Привлечь ведущих экспертов для обеспечения того, чтобы планы соответствовали передовой практике и поставленной цели.
4. Опираться на данные, полученные от деловых кругов и гражданского общества.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

1 Возможности вовлеченных организаций

E **Выявить заинтересованные стороны в области безопасности детей в Интернете.**

Возможно, имеет смысл объединить заинтересованные стороны в группу с формальной ролью поддержки и информирования Руководящего комитета. в качестве альтернативы может оказаться более практичным взаимодействие с заинтересованными сторонами на более неформальной основе или по мере необходимости. в любом случае вполне вероятно, что будет существовать большая группа «заинтересованных сторон», включая родителей/опекунов, учителей и детей, и меньшая группа людей с соответствующими навыками и опытом, в которую могут войти представители правоохранительных органов, отрасли, эксперты по правам ребенка, НПО (как национальные, так и международные), медицинские работники и представители научных кругов. Использование их интересов и опыта может быть очень полезным для продвижения или реализации политики безопасности детей в Интернете в различных контекстах.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Составить список заинтересованных сторон и носителей навыков и опыта, которые охватывают все области политики, перечисленные в Наборе программных средств. Подсказки см. в шаблоне, приведенном в разделе Средства поддержки 2 (стр. 49).
2. Убедиться, что они включают детей или представителей, которые работают непосредственно с детьми.
3. Если это формальная группа, определить круг полномочий, который четко обязывает группу заинтересованных сторон участвовать в деятельности Руководящего комитета.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

1 Возможности вовлеченных организаций

F **Определить роли и обязанности**

Должна существовать совместная нормативно-правовая база, определяющая роли и обязанности всех организаций, разрабатывающих цифровую инфраструктуру, сети и сервисы, а также управляющих ими, и обязанности государственных ведомств. Следует установить минимальные стандарты для всех участников цепочки создания стоимости, включая тех, кто отвечает за инфраструктуру, аппаратные средства и цифровые продукты и услуги, а также тех, кто управляет ими или использует их при взаимодействии с детьми. Эти стандарты должны быть сосредоточены на безопасности детей и полной реализации их прав в цифровом мире. Следует обеспечить участие гражданского общества в группах заинтересованных сторон.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Определить четкую сферу ответственности за каждое из действий в вашем плане.
2. Составить карту различных ведомств, государственных, регулирующих или профильных организаций, школ, благотворительных организаций, медицинских учреждений и предприятий, несущих ответственность, чтобы обеспечить охват, прозрачность и подотчетность по всем аспектам.

G **Определить показатели эффективности и систему оценки**

Для каждого аспекта плана реализации нужно определить соответствующий ответственный орган (лицо, учреждение, ведомство) и людские и финансовые ресурсы для успешного выполнения поставленной задачи. Один и тот же орган может отвечать сразу за несколько областей политики или только за одну из них. Чтобы Руководящий комитет мог осуществлять надзор и отслеживать прогресс, следует внедрить ключевые показатели эффективности (KPI), механизмы оценки и четкие структуры отчетности. в связи с быстрым развитием цифровой среды KPI необходимо постоянно пересматривать.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Установить KPI и процессы анализа в рамках стратегического плана. Например, KPI, изложенные в документе «Защита детей в Интернете, Руанда».[77]
2. Установить четкие границы ответственности для Руководящего комитета.

77. Защита детей в Интернете, Руанда, Фонд 5Rights, 2019 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

1 Возможности вовлеченных организаций

H **Обеспечить интеграцию вопросов безопасности детей в Интернете во все области государственной политики**

Любые профильные национальные планы, такие как Национальный план развития широкополосной связи, Национальный план действий по борьбе с насилием в отношении детей (VAC), программа обеспечения компьютерной грамотности, стратегия кибербезопасности и т. д., должны включать политику обеспечения безопасности детей в Интернете в качестве составной части стратегии внедрения. Планы, которые осуществляются в течение нескольких лет, должны пересматриваться и обновляться на ключевых этапах.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Использовать контрольный перечень, приведенный в разделе Средства поддержки 3, чтобы проанализировать области политики и определить, включена ли в них безопасность детей в Интернете (стр. 51). Возможно, имеет смысл привлечь внешнего эксперта для сверки стратегического плана с существующей государственной политикой и положениями.
2. Довести информацию об отклонениях от нормы до сведения Национального руководящего комитета по безопасности детей в Интернете, созданного в процессе D.

Как это согласуется с основополагающими документами

Правительства должны создать национальную координационную структуру с четким мандатом и достаточными полномочиями для координации всех мероприятий, связанных с правами детей и цифровыми СМИ и ИКТ на межсекторальном, национальном, региональном и местном уровнях. Правительства должны включить цели с конкретными сроками и прозрачный процесс оценки и мониторинга прогресса, а также обеспечить выделение необходимых людских, технических и финансовых ресурсов для эффективного функционирования этой структуры.

Правительствам следует создать многостороннюю платформу для руководства разработкой, осуществлением и мониторингом национальной цифровой повестки дня для детей. Такая платформа должна объединять представителей наиболее важных групп, включая детей и молодежь, ассоциации родителей/опекунов, соответствующие правительственные органы, секторы образования, правосудия, здравоохранения и социального обеспечения, национальные правозащитные учреждения и соответствующие регулирующие органы, гражданское общество, отрасль, научные круги и соответствующие профессиональные ассоциации.

Источник: Руководящие указания для директивных органов по защите ребенка в онлайновой среде, Международный союз электросвязи, 2020 г.[78]

78. Руководящие указания для директивных органов по защите ребенка в онлайновой среде, Международный союз электросвязи, 2020 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

Средства поддержки

1. **Шаблон SWOT-анализа для выявления наиболее подходящего ведущего департамента или министерства**

Процесс B («Выберите министерство или ведомство, которое возьмет на себя ведущую роль при разработке национальной политики безопасности детей в Интернете») предполагает тщательный выбор наиболее подходящего ведущего ведомства по безопасности детей в Интернете. Данный инструмент призван упростить для вас этот процесс.

Разные страны применяют различные подходы при выборе ведущего ведомства, например:

- **Танзания** – Министерство здравоохранения
- **Гана** – Министерство связи
- **Эфиопия** – Надзорный орган
- **Австралия** – Министерство инфраструктуры, транспорта, регионального развития и связи
- **Великобритания** – Министерство по вопросам цифровых технологий, культуры, СМИ и спорта

Чтобы определить, какое из министерств и ведомств лучше всего подходит для того, чтобы возглавить работу по обеспечению безопасности детей в Интернете, проведите SWOT-анализ (сильные и слабые стороны, возможности и угрозы) каждого потенциального министерства или ведомства:

Сильные стороны	Слабые стороны
Что нужно учесть: есть ли у этого министерства особо сильные стороны в области обеспечении безопасности в Интернете? Входит ли уже какая-либо из областей применения политики в сферу обязанностей министерства? Достаточно ли у него ресурсов для выполнения ведущей роли? Достаточно ли у него связей и влияния для выполнения этой работы? Готово ли и способно ли его руководство взять на себя эту задачу?	**Что нужно учесть:** есть ли у этого министерства особо слабые стороны в области обеспечения безопасности в Интернете? Хватит ли ему потенциала или возможностей для выполнения дополнительных обязанностей? Хватит ли ему связей или влияния для выполнения этой межсекторальной задачи? Готово ли руководство взять на себя задачу и хватит ли ему организаторских способностей?
Возможности	**Угрозы**
Что нужно учесть: существует ли синергия между задачей обеспечения безопасности детей в Интернете и новыми политическими задачами в этом министерстве (например, широкополосная связь или развертывание 5G)? Укомплектовано ли это министерство государственными служащими или политиками, которые могут оказаться более эффективны, чем другие?	**Что нужно учесть:** достаточно ли эффективно министерство выполняет уже существующие задачи? Существуют ли какие-либо угрозы для министерства (например, ожидаемое сокращение бюджета)? Есть ли у министерства какие-либо конкурирующие интересы, которые могут помешать ему взять на себя ведущую роль (например, конфликтующее финансирование или действующие соглашения с поставщиками телекоммуникационных услуг или технологическими компаниями)? Существуют ли планы замены руководства?

2. Шаблон для выявления заинтересованных сторон

Этот шаблон поможет вам составить список заинтересованных сторон для создания группы заинтересованных сторон, с указанием их ролей и обязанностей, как того требует процесс E («Выявить заинтересованные стороны в области безопасности детей в Интернете»). Представители, организации, их роли и обязанности будут зависеть от местного контекста, и их может быть несколько для каждого типа. После того как вы определились с подходящим ведущим министерством или организацией, важно также включить в процесс те же или аналогичные заинтересованные стороны, чтобы обеспечить равновесие, эффективность и надлежащее исполнение.

Перечисленные ниже типы отражают типы, указанные в Руководящих указаниях для директивных органов по защите ребенка в онлайновой среде Международного союза электросвязи 2020 г., а также типы, упомянутые в Замечании общего порядка № 25 (2021 г.).

Представитель заинтересованной стороны	Тип	Организация	Роль и обязанности
Пример: Назначенное лицо или представитель с соответствующими полномочиями для участия, принятия решений, распределения ресурсов	Дети и молодежь	Молодежная группа X	Голос ребенка: дать представление о проблеме с точки зрения детей; выделить проблемы и вопросы детей
	Молодежная консультативная группа 5Rights		Голос ребенка: дать представление о проблеме с точки зрения детей; выделить проблемы и вопросы детей
	Родители, опекуны, педагоги		Обеспечение поддержки в политике взрослых, осуществляющих уход за детьми
	Представители отрасли		Обеспечение того, чтобы политика обязывала все продукты и услуги быть ориентированными на детей и безопасными
	Научное сообщество и НПО		Обеспечение отражения в политике современных данных и опыта

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

1 Возможности вовлеченных организаций

Представитель заинтересованной стороны	Тип	Организация	Роль и обязанности
	Правоохранительные органы		Обеспечение того, чтобы политика имела правовое обеспечение и предполагала просвещение сотрудников правоохранительных органов
	Социальные службы		Обеспечение того, чтобы политика учитывала интересы уязвимых детей
	Здравоохранение		Отражение медицинских рекомендаций и поддержка жертв киберпреступлений и/или тех, кто подвергается риску или вреду
	Государственные министерства и регулирующие органы		Привлечение специализированных регулирующих органов и министерств, за исключением ведущего министерства
	Операторы широкополосных, мобильных и Wi-Fi сетей		Поддержка безопасного и недорогого цифрового доступа для детей
	Организации по защите прав детей		Обеспечение осуществления и реализации всего спектра прав детей в цифровой политике
	Ученые, юристы, частные лица, организации с конкретным опытом, например, в области права, алгоритмического аудита, модерирования и т. д.		Предоставление специализированной помощи «по мере необходимости», чтобы обеспечить продуманную, но в то же время практичную политику

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

3. Контрольный список для определения того, какие области политики касаются безопасности детей в Интернете

Этот контрольный список поможет вам проанализировать существующие политики, чтобы определить, содержит ли каждая из них аспекты безопасности детей в Интернете. Это поможет вам перейти к процессу H («Обеспечить интеграцию вопросов безопасности детей в Интернете во все области государственной политики»).

Уведомите группу заинтересованных сторон по безопасности детей в Интернете о результатах этого анализа.

Элемент безопасности детей в Интернете, включенный в политику безопасности детей в Интернете	Отметьте уже включенные	Для еще не включенных определите недостатки, отклонения от нормы и рекомендуемые изменения и сообщите об этом группе заинтересованных сторон по безопасности детей в Интернете
Национальный план развития широкополосной связи	☐	
Рамки и планы мероприятий для реализации Целей устойчивого развития	☐	
Все необходимые образовательные и учебные программы	☐	
Концепции компьютерной грамотности для детей	☐	
Национальная образовательная программа для школ	☐	
Программа профессиональной подготовки преподавателей и социальных работников	☐	
Программа профессиональной подготовки сотрудников полиции и правоохранительных органов	☐	

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

1 Возможности вовлеченных организаций

Элемент безопасности детей в Интернете, включенный в политику безопасности детей в Интернете	Отметьте уже включенные	Для еще не включенных определите недостатки, отклонения от нормы и рекомендуемые изменения и сообщите об этом группе заинтересованных сторон по безопасности детей в Интернете
Права потребителей	☐	
Насилие в отношении детей, стратегия защиты и охраны детей	☐	
Уголовное правосудие	☐	
Права человека	☐	
Организации по защите	☐	
Равенство и борьба с дискриминацией	☐	
Защита данных	☐	
Международная торговля	☐	
Контроль над азартными играми	☐	

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

1 Возможности вовлеченных организаций

Элемент безопасности детей в Интернете, включенный в политику безопасности детей в Интернете	Отметьте уже включенные	Для еще не включенных определите недостатки, отклонения от нормы и рекомендуемые изменения и сообщите об этом группе заинтересованных сторон по безопасности детей в Интернете
Стандарты в области рекламы	☐	
Финансовые преступления	☐	
Образовательные программы	☐	
Здравоохранение	☐	
Международное сотрудничество	☐	
Другие	☐	

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

Прочие справочные ресурсы

1. Совет по безопасности в Интернете Великобритании (UKCIS) как модель группы заинтересованных сторон по обеспечению безопасности детей в Интернете[79]

Совет по безопасности в Интернете Великобритании (UKCIS) — это совместный форум, в рамках которого сотрудничают правительство, технологическое сообщество и третий сектор. UKCIS входит в состав Министерства цифровых технологий, культуры, СМИ и спорта, Министерства образования и Министерства внутренних дел. с течением времени UKCIS стал местом встреч для предпринимателей, ученых, экспертов по детской безопасности, государственных служащих и министров. Он также заказал проведение важных исследований, которые послужили доказательной базой для разработки политики. в отличие от рекомендации, содержащейся в Наборе программных средств, UKCIS официально не был подключен к плану действий для руководящей группы.

2. Руководство МСЭ по разработке национальной стратегии кибербезопасности — стратегическое участие в кибербезопасности[80]

При содействии МСЭ двенадцать партнеров из государственного и частного секторов, научных кругов и гражданского общества делятся своим опытом, знаниями и компетенциями, предоставляя обобщенный, согласованный набор принципов по разработке, созданию и реализации национальных стратегий кибербезопасности. Целью данного руководства является стимулирование стратегического мышления и оказание помощи национальным лидерам и законодателям в разработке, создании и осуществлении национальных стратегий кибербезопасности во всем мире.

3. Руководство Совета Европы для законодателей по правам ребенка в цифровой среде[81]

Данное руководство направлено на поддержку государств-членов Совета Европы в реализации Рекомендации CM/Rec(2018)7 и руководящих принципов по соблюдению, защите и реализации прав ребенка в цифровой среде. Этот документ содержит первые в мире всеобъемлющие руководящие принципы для государств в отношении прав детей в цифровой среде.

4. Защита детей в Интернете, Руанда[82]

Созданная в партнерстве между Фондом 5Rights, Университетом Восточного Лондона, Университетом Руанды и правительством Руанды, Политика защиты детей в Интернете предлагает план реализации на высшем уровне в качестве примера для любого государства, заинтересованного вопросами безопасности детей в Интернете.

79. Совет Великобритании по безопасности в Интернете, Министерство цифровой культуры, СМИ и спорта, Министерство образования и Министерство внутренних дел, 2021 г.
80. Руководство по разработке национальной стратегии кибербезопасности — стратегическое участие в кибербезопасности, Международный союз электросвязи, 2018 г.
81. Руководство для законодателей по правам ребенка в цифровой среде, Совет Европы, 2020 г.
82. Защита детей в Интернете, Руанда, Фонд 5Rights, 2019 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

2 Нормативно-правовое регулирование

> **Дети могут столкнуться с особыми трудностями при получении средств правовой защиты, если их права нарушаются в цифровой среде предприятиями, особенно в контексте их глобальной деятельности. Государства-участники должны рассмотреть меры по соблюдению, защите и реализации прав детей в контексте экстерриториальной деятельности предприятий при условии, что существует разумная связь между государством и соответствующим поведением. Они должны обеспечить предоставление предприятиями эффективных механизмов подачи и рассмотрения жалоб; однако такие механизмы не должны препятствовать доступу детей к государственным средствам правовой защиты. Они также должны обеспечить, чтобы ведомства, обладающие надзорными полномочиями, имеющие отношение к правам детей, например, в области здравоохранения и безопасности, защиты данных и прав потребителей, образования, рекламы и маркетинга, расследовали жалобы и предоставляли адекватные средства правовой защиты в случае нарушений или злоупотреблений правами детей в цифровой среде.**
>
> Источник: Замечание общего порядка № 25 (2021 г.), п. 48[83]

Цель

Усилить и привести в соответствие национальные правовые и нормативные режимы в отношении безопасности детей в Интернете, а также укрепить потенциал и возможности правоохранительных органов и регулирующих органов в области безопасности детей в Интернете, включая возможность сотрудничать с другими секторами, в частности, с сектором ИКТ.

Текст типовой политики

Для обеспечения целостного подхода к безопасности детей в Интернете необходимо предпринять следующие шаги.

2a. Ужесточать законы, запрещающие правонарушения в области безопасности детей в Интернете, и обеспечивать соблюдение таких законов
Уголовное законодательство и процедуры способствуют расследованию и судебному преследованию киберпреступлений, нарушающих право детей на защиту, и должны быть усилены и изменены в соответствии с международными стандартами и передовой практикой. Речь идет о введении обязательной оценки рисков для снижения потенциального вреда, а также, при необходимости, усилении ответственности и наказании. Также необходимо включить процедуры уведомления о нежелательном контенте и его удаления. Уголовное законодательство, касающееся безопасности детей в Интернете, должно разрабатываться с учетом всех прав ребенка, включая право быть выслушанным и право на участие.[84]

83. Замечание общего порядка № 25 (2021 г.) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.
84. Например, нормативно-правовые акты, не дающие четкого представления о том, могут ли самостоятельно созданные сексуальные изображения, которыми обмениваются дети по взаимному согласию, считаться незаконными материалами по сексуальным надругательствам над детьми. Даже если дети не подвергаются судебному преследованию на практике, такая юридическая неопределенность с потенциальной криминализацией может подорвать их доверие, контроль и права на самостоятельность.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

2 Нормативно-правовое регулирование

2b. Ввести правила защиты данных и создать независимые органы надзора, обеспечивающие надлежащую защиту данных детей и их сбор только в случае необходимости и с высоким уровнем безопасности

Такие общие правила должны предусматривать особую категорию для детских данных, автоматически требующую более высокого уровня защиты и гарантий, а также защиту от ненадлежащего коммерческого использования данных о детях. в тех случаях, когда у детей или родителей/опекунов запрашивается согласие на сбор и обработку данных о несовершеннолетних, такое согласие должно быть информированным и осознанным. Сбор данных в целях обеспечения безопасности должен рассматриваться в исключительных обстоятельствах, когда это соответствует интересам ребенка.

2c. Усилить уголовное расследование, преследование и наказание за сексуальную эксплуатацию детей или жестокое обращение с ними в Интернете[85]

Сотрудники уголовной юстиции, занимающиеся правонарушениями, связанными с безопасностью детей в Интернете, должны пройти обучение в этой области в целях содействия более активному предупреждению, успешному судебному преследованию, вынесению надлежащего наказания, а также более глубокому пониманию последствий для жертв. Следует пересмотреть и укрепить потенциал следственных групп и оперативников в целях выявления, предотвращения и реагирования на угрозы кибербезопасности, особенно когда они связаны с безопасностью детей в Интернете. Системы уголовной юстиции должны быть в состоянии обеспечить своевременный доступ к правосудию.

2d. Оценить и укрепить системы ювенальной юстиции

Обеспечить ясность и соразмерность законодательства для сведения к минимуму риска нарушения закона со стороны ребенка в контексте безопасности детей в Интернете. в тех случаях, когда ребенок сталкивается с уголовным наказанием, связанным с безопасностью детей в Интернете, например, в связи с кибербуллингом или сексуальными надругательствами на основе изображений, система правосудия должна прилагать все усилия для предотвращения криминализации детей и обеспечивать надлежащую поддержку и юридическое представительство нарушителей для защиты их прав.

2e. Выявить и ратифицировать международные договоры и протоколы, касающиеся безопасности детей в Интернете

Создание устойчивой экосистемы безопасности детей в Интернете требует подхода с участием многих заинтересованных сторон и глобального взаимодействия. Каждая страна должна определить и ратифицировать соответствующие международные и региональные протоколы и договоры, а также предпринять шаги по осуществлению приведенных в них мер.

2f. Укрепить потенциал правоохранительных органов

Недостатки в правоприменении и судебной системе должны быть выявлены, и меры должны быть приняты для улучшения информированности, отчетности и успешного судебного преследования. По возможности следует стремиться к организации международной подготовки кадров и обмену опытом, а также поощрять межсекторальную координацию и сотрудничество между отраслью и правоохранительными органами.

85. Под сексуальной эксплуатацией детей и жестоким обращением с ними (CSEA) подразумеваются случаи, когда ребенка принуждают или убеждают принять участие в сексуальных действиях. Речь может идти о физическом контакте или бесконтактных действиях, и такие действия могут происходить в Интернете или за его пределами.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

2 Нормативно-правовое регулирование

План мероприятий для достижения цели

A **Ужесточать законы, запрещающие правонарушения в области безопасности детей в Интернете, и обеспечивать соблюдение таких законов**

Уголовное законодательство и процедуры способствуют расследованию и судебному преследованию киберпреступлений, нарушающих право детей на защиту, и должны быть усилены и изменены в соответствии с международными стандартами и передовой практикой. Речь идет о введении обязательной оценки рисков для снижения потенциального вреда, а также, при необходимости, усилении ответственности и наказания. Также необходимо включить процедуры уведомления о нежелательном контенте и его удаления. Уголовное законодательство, касающееся безопасности детей в Интернете, должно разрабатываться с учетом всех прав ребенка, включая право быть выслушанным и право на участие.[86]

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Выявить соответствующие законы. Подсказки см. в контрольном списке, приведенном в разделе Средства поддержки 1 (стр. 64).
2. Проверить их соответствие международным стандартам в каждой из областей, например, ювенальная юстиция и т. д.
3. Провести оценку рисков по существующему законодательству.
4. Заказать экспертам анализ недочетов.
5. Предложить поправки к существующим законам.
6. Запланировать информационно-пропагандистские меры для обеспечения принятия поправок и наличия необходимых ресурсов для их применения.

86. Например, нормативно-правовые акты, не дающие четкого представления о том, могут ли самостоятельно созданные сексуальные изображения, которыми обмениваются дети по взаимному согласию, считаться незаконными материалами по сексуальным надругательствам над детьми. Даже если дети не подвергаются судебному преследованию на практике, такая юридическая неопределенность с потенциальной криминализацией может подорвать их доверие, контроль и права на самостоятельность.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

2 Нормативно-правовое регулирование

B **Установить правила защиты данных и создать независимые органы надзора, обеспечивающие надлежащую защиту данных детей и их сбор только в случае необходимости и с высоким уровнем безопасности**

В некоторых юрисдикциях существует общее законодательство о защите данных, которое, возможно, нуждается в совершенствовании или формализации для обеспечения детям защиты, соответствующей их возрасту. в других странах, где защита данных отсутствует или ее недостаточно, может возникнуть необходимость в разработке законодательства о защите данных исключительно для детей. в обоих случаях данные о детях должны выделяться в особую категорию, автоматически требующую более высокого уровня защиты и гарантий, а также защиты от ненадлежащего коммерческого использования данных о детях. в тех случаях, когда у детей или родителей/опекунов запрашивается согласие на сбор и обработку данных о несовершеннолетних, такое согласие должно быть информированным и осознанным. в исключительных обстоятельствах, когда это отвечает интересам ребенка, особое внимание следует уделять сбору данных в целях обеспечения безопасности.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Провести анализ недочетов в существующей нормативно-правовой базе по защите данных.
2. Предложить новые правила или поправки с ресурсами и доказательствами для их поддержки.
3. Создать или задействовать уже существующие независимые надзорные органы для мониторинга и обеспечения соответствия.
4. Привести защиту данных о детях в соответствие с существующей международной практикой.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

2 Нормативно-правовое регулирование

C **Усилить уголовное расследование, преследование и наказание за сексуальную эксплуатацию детей или жестокое обращение с ними в Интернете**[87]

Сотрудники уголовной юстиции, занимающиеся правонарушениями, связанными с безопасностью детей в Интернете, должны пройти обучение в этой области в целях содействия более активному предупреждению, успешному судебному преследованию, вынесению надлежащего наказания, а также более глубокому пониманию последствий для жертв. Следует пересмотреть и укрепить потенциал следственных групп и оперативников в целях выявления, предотвращения и реагирования на угрозы киберугрозы или злоупотребления, связанные с безопасностью детей в Интернете. Системы уголовной юстиции должны быть в состоянии обеспечить своевременный доступ к правосудию.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Включить в учебную программу вопросы безопасности детей в Интернете (см. руководства и ресурсы в пункте «Обучение» раздела «Область применения политики» на стр. 144).
2. Проанализировать навыки и пробелы, связанные с безопасностью детей в Интернете.
3. Выполнить обзор ресурсов для обеспечения эффективного доступа к правосудию, ориентированному на ребенка.

87. Под сексуальной эксплуатацией детей и жестоким обращением с ними (CSEA) подразумеваются случаи, когда ребенка принуждают или убеждают принять участие в сексуальных действиях. Речь может идти о физическом контакте или бесконтактных действиях, и такие действия могут происходить в Интернете или за его пределами.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

2 Нормативно-правовое регулирование

D **Оценить и укрепить системы ювенальной юстиции**

Обеспечьте ясность и соразмерность законодательства для сведения к минимуму риска нарушения закона со стороны ребенка в контексте безопасности детей в Интернете. в тех случаях, когда ребенок сталкивается с уголовным наказанием, связанным с безопасностью детей в Интернете, например, в связи с кибербуллингом или сексуальными надругательствами на основе изображений, система правосудия должна прилагать все усилия для предотвращения криминализации детей и обеспечивать надлежащую поддержку и юридическое представительство нарушителей для защиты их прав.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Провести оценку и анализ недочетов в системе ювенальной юстиции.
2. Предложить поправки, где это необходимо.
3. Провести работу по развитию компетенций ключевых специалистов и подумать о стратегиях профилактики и повышения осведомленности в целях снижения риска криминализации.

E **Выявить и ратифицировать международные договоры и протоколы, касающиеся безопасности детей в Интернете.**

Создание устойчивой экосистемы безопасности детей в Интернете требует подхода с участием многих заинтересованных сторон и глобального взаимодействия. Каждая страна должна определить и ратифицировать соответствующие международные и региональные протоколы и договоры, а также предпринять шаги по осуществлению приведенных в них мер.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Просмотреть ресурсы в Приложении D.
2. Перечислить соответствующие документы.
3. Выявить любые препятствия на пути ратификации.
4. Разработать предложения по подписанию и ратификации.
5. Подписать и ратифицировать документы.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

2 Нормативно-правовое регулирование

F **Укрепить потенциал правоохранительных органов**

Нужно выявить недостатки в правоприменении и судебной системе и принять меры для улучшения информированности и отчетности и успешного судебного преследования. По возможности следует стремиться к организации международной подготовки кадров и обмену опытом, а также поощрять межсекторальную координацию и сотрудничество между представителями отрасли и правоохранительными органами.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Выявить пробелы в навыках.
2. Определить учебные модули (см. руководства и ресурсы в пункте «Обучение» раздела «Область применения политики» на стр. 144).
3. Определить возможных национальных и международных партнеров для обмена навыками (см. раздел Применение политики в области Международного сотрудничества за ресурсы, стр. 161).

Как это согласуется с основополагающими документами

«Законы и нормативные акты являются важными инструментами для обеспечения того, чтобы деятельность и деловые операции предприятий не оказывали негативного воздействия на права детей и не нарушали их. Государствам следует принять законодательство, обеспечивающее соблюдение прав ребенка третьими сторонами и предусматривающее четкие и предсказуемые правовые и нормативные рамки, позволяющие предприятиям соблюдать права детей».

Замечание общего порядка № 16 (2013 г.) об обязательствах государств в отношении воздействия предпринимательского сектора на права детей, п. 53[88]

Несмотря на существование внутренних механизмов рассмотрения жалоб, правительствам следует создать механизмы мониторинга для расследования нарушений прав детей и возмещения ущерба с целью повышения подотчетности компаний, работающих в сфере ИКТ, и других компаний, а также усилить ответственность регулирующих органов за разработку стандартов, касающихся прав детей и ИКТ. Это особенно важно, поскольку другие средства правовой защиты, доступные пострадавшим от действий корпорации, такие как гражданское судопроизводство и другие средства судебной защиты, часто являются сложными и дорогостоящими.

Источник: Руководящие указания для директивных органов по защите ребенка в онлайновой среде, Международный союз электросвязи, 2020 г.[89]

88. Замечание общего порядка № 16 (2013 год) об обязательствах государств в отношении воздействия предпринимательского сектора на права детей, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2013 г.
89. Руководящие указания для директивных органов по защите ребенка в онлайновой среде, Международный союз электросвязи, 2020 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

Средства поддержки

1. Контрольный список законодательных актов: пример

Это поможет вам выявить соответствующие законы и политики в вашей юрисдикции в рамках выполнения процесса А («Ужесточать законы, запрещающие правонарушения в области безопасности детей в Интернете, и обеспечивать соблюдение таких законов»). Примеры из Великобритании являются ознакомительными и должны быть заменены соответствующими национальными или региональными примерами.

Область политики	Законодательство/ правовое регулирование	Статус	Включает безопасность детей в Интернете?	Регулирующий орган/суд
Права потребителей	Закон о правах потребителей 2015 г.[90] Нормы безопасности игрушек 2011 г.[91] Общие нормы безопасности продукции 2005 г.[92]	Закон Нормативный документ Нормативный документ	Да	Суд
Защита детей	Закон о детях и социальной работе 2017 г.[93] Закон о детях 2004 г.[94] Закон о цифровой экономике 2017 г.[95]	Закон Закон Закон	Да	Суд по семейным делам
Уголовное правосудие	Различные правонарушения в рамках уголовного законодательства	Закон	Да	Суд
Права человека, включая права ребенка	Закон о правах человека 1998 г.[96] Конвенция ООН о правах ребенка[97] Замечание общего порядка № 25 (2021 г.) о правах детей в отношении цифровой среды[98]	Закон Соглашение Соглашение	Да	Суд Комиссия по вопросам равенства и правам человека (и национальные комиссии) Отчетность перед Комитетом ООН по правам ребенка Судебные органы ООН

90. Закон о правах потребителей 2015, Глава 3 «Цифровой контент», Великобритания; Закон о правах потребителей (Цифровой контент) Руководство для бизнеса, Министерство по делам предпринимательства, инноваций и профессионального образования, 2015 г.
91. Нормы безопасности игрушек 2011 г., Управление по безопасности и стандартам продукции, 2011 г.
92. Общие нормы безопасности продукции 2005 года, Правительство Великобритании, 2017 г.
93. Закон о детях и социальной работе 2017 г., глава 2 «Защита детей», Правительство Великобритании, 2004 г.
94. Закон о детях 2004 г., Правительство Великобритании, 2004 г.
95. Закон о цифровой экономике 2017 г., Правительство Великобритании, 2017 г.
96. Закон о правах человека 1998 г., Правительство Великобритании, 1998 г.
97. Конвенция о правах ребенка, Управление Верховного комиссара Организации Объединенных Наций по правам человека, 1989 г.
98. Замечание общего порядка № 25 (2021 г.) о правах детей в отношении цифровой среды, Комитет Организации Объединенных Наций по правам ребенка, 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

2 Нормативно-правовое регулирование

Область политики	Законодательство/ правовое регулирование	Статус	Включает безопасность детей в Интернете?	Регулирующий орган/суд
Защита данных	Нормы проектирования с учетом возраста 2020 г.[99] Закон о защите данных 2018 г.[100]	Закон Закон	Да	Управление Комиссара по вопросам информации
Международная торговля	Закон о торговле 2021 г.[101] (добавлено положение о защите детей)	Закон	Да	Суд
Азартные игры	Закон об азартных играх 2005 г.[102]	Закон	Да	Комиссия по азартным играм
Реклама	Комитет рекламных стандартов, Кодекс неэфирной рекламы и прямого и рекламного маркетинга 2010 г.[103] Комитет рекламных стандартов, Кодекс эфирной рекламы 2010 г.[104]	Необязательный Необязательный	Да	Членская организация с совместным регулированием под эгидой Ofcom
Финансовые преступления	Закон о мошенничестве 2006 г.[105] Закон о воровстве 1968 г.[106] Закон о доходах, полученных преступным путем 2002 г.[107] Положения об отмывании денег, финансировании терроризма и переводе средств (информация о плательщике) 2017 г.[108] Закон о санкциях и борьбе с отмыванием денег 2018 г.[109]	Закон Закон Закон Закон Закон	Нет, но существует необязательный кодекс этических норм эмитентов кредитных карточек в отношении CSEA и порнографии	Суд Суд Суд Управление по регулированию и надзору в сфере финансовых услуг Управление по регулированию и надзору в сфере финансовых услуг

99. Нормы проектирования с учетом возраста 2020 года, Правительство Великобритании, 2020 г.
100. Закон о защите данных 2018 года, Правительство Великобритании, 2018 г.
101. Закон о торговле 2021 года, Правительство Великобритании, 2021 г.
102. См. Закон об азартных играх 2005 года, часть 1, раздел 4 (Дистанционные азартные игры) и часть 4 (Защита детей и молодежи) 2005 года, Правительство Великобритании, 2005 г.
103. См. Кодекс неэфирной рекламы и прямого и рекламного маркетинга, Раздел 5 (Дети), Комитет рекламных стандартов, 2010 г.
104. См. Кодекс эфирной рекламы, Раздел 5 (Дети), Комитет рекламных стандартов, 2010 г.
105. Закон о мошенничестве 2006 года, Правительство Великобритании, 2006 г.
106. Закон о кражах 1968 года, Правительство Великобритании, 1968 г.
107. Закон о доходах от преступной деятельности 2002 года, Правительство Великобритании, 2002 г.
108. Положения об отмывании денег, финансировании терроризма и переводе средств (информация о плательщике) 2017 года, Правительство Великобритании, 2017 г.
109. Закон о санкциях и борьбе с отмыванием денег 2018 года, Правительство Великобритании, 2018 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

2 Нормативно-правовое регулирование

Область политики	Законодательство/ правовое регулирование	Статус	Включает безопасность детей в Интернете?	Регулирующий орган/суд
Образовательные программы	Закон о детях и социальной работе 2017 г.[110] Конвенция ООН о правах ребенка[111] Замечание общего порядка № 25 (2021 г.) о правах детей в отношении цифровой среды[112]	Закон Соглашение Соглашение	Да	Суд, Комитет по стандартам в сфере образования Отчетность перед Комитетом ООН по правам ребенка
Здравоохранение	Закон о здравоохранении и социальной помощи 2012 г.[113]	Закон	Нет	Главный врач Суд Суд по семейным делам
Международное сотрудничество	Цели в области устойчивого развития[114]	Международное соглашение	Нет	Суд
Равенство	Закон о равенстве 2010 г.[115]	Закон	Нет	Суд Комиссия по вопросам равенства и правам человека и национальные комиссии в автономных странах

110. Закон о детях и социальной работе 2017 года, Правительство Великобритании, 2017 г. (особенно глава 4 об отношениях, сексе и санитарно-медицинском просвещении).
111. Конвенция о правах ребенка, Управление Верховного комиссара Организации Объединенных Наций по правам человека, 1989 г.
112. Замечание общего порядка № 25 (2021 г.) о правах детей в отношении цифровой среды, Комитет Организации Объединенных Наций по правам ребенка, 2021 г.
113. Закон о здравоохранении и социальной помощи 2012 г., Правительство Великобритании, 2012 г.
114. Преобразование нашего мира: Повестка дня в области устойчивого развития на период до 2030 года, Организация Объединенных Наций, 2021 г.
115. Закон о равенстве 2010 года, Правительство Великобритании, 2010 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

2. Контрольный список законодательных актов для заполнения

Это поможет вам выявить соответствующие законы и политики в вашей юрисдикции в рамках выполнения процесса А («Ужесточать законы, запрещающие правонарушения в области безопасности детей в Интернете, и обеспечивать соблюдение таких законов»).

Область политики	Законодательство/ правовое регулирование	Статус	Включает безопасность детей в Интернете?	Регулирующий орган/суд
Права потребителей				
Защита детей				
Уголовное правосудие				
Права человека, включая права ребенка				
Защита данных				
Планы развития широкополосной связи				
Международная торговля				

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

2 Нормативно-правовое регулирование

Область политики	Законодательство/ правовое регулирование	Статус	Включает безопасность детей в Интернете?	Регулирующий орган/суд
Азартные игры				
Реклама				
Финансовые преступления				
Образовательные программы				
Здравоохранение				
Международное сотрудничество				
Равенство				
Другое				

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

Прочие справочные ресурсы

1. Тематическое исследование, посвященное надзорным механизмам в Албании[116]

Национальный совет по правам и защите ребенка был учрежден в законодательном порядке в качестве подотчетного национального комитета по управлению и надзору; защита детей от сексуальной эксплуатации и жесткого обращения с ними в Интернете включена в основные политики и законодательные акты.

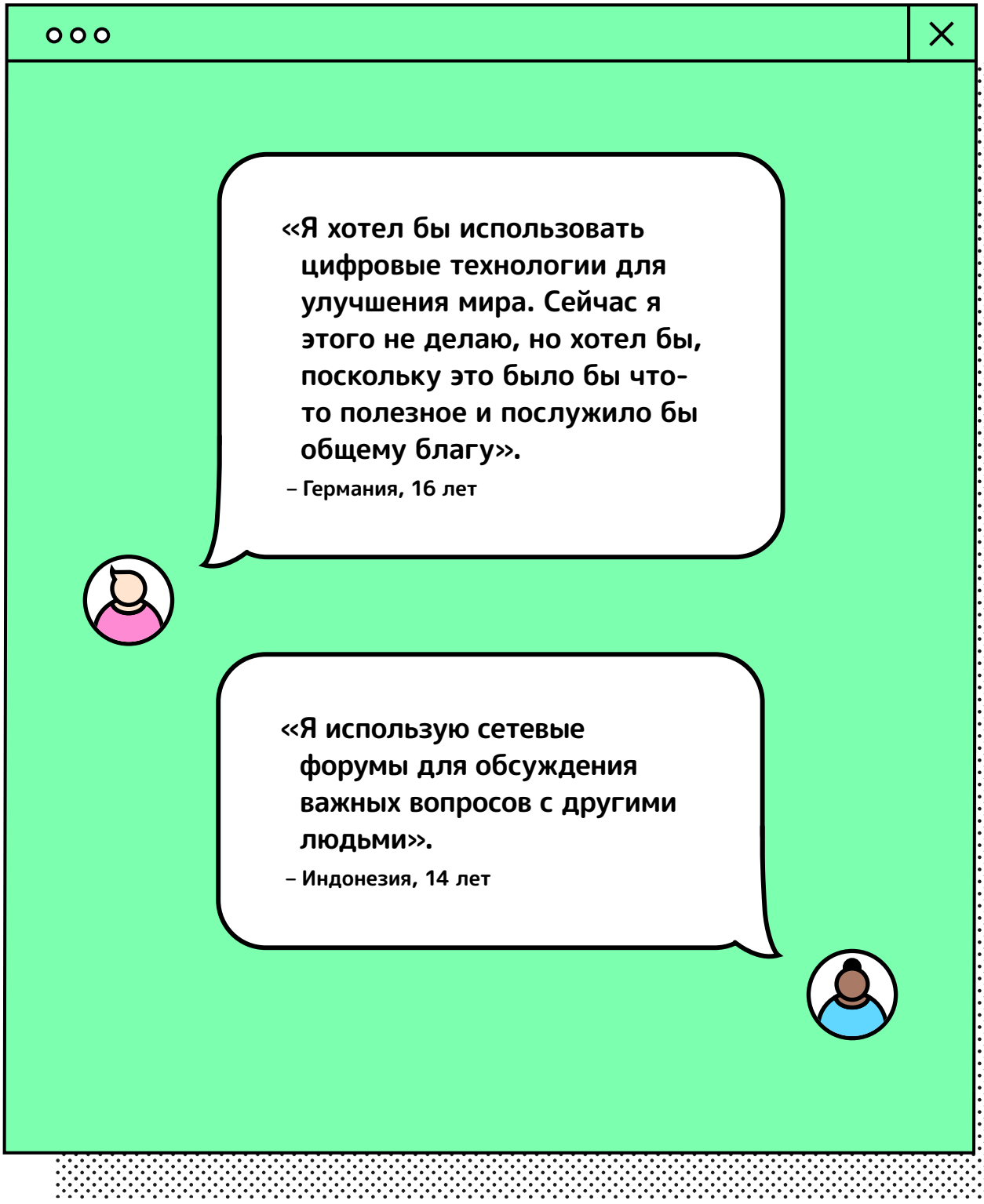
2. Закон Ганы о кибербезопасности (Закон 1038)[117]

Закон Ганы о кибербезопасности (Закон 1038) содержит положения о защите детей в Интернете путем криминализации сексуальных действий с участием детей в Интернете. Непристойные изображения и фотографии детей, обольщение детей с целью сексуального насилия, киберпреследование и сексуальное вымогательство запрещены законом. Закон налагает на провайдеров телекоммуникационных услуг определенные обязательства по защите детей в цифровом пространстве. в Закон о детях (Закон 560) были предложены поправки.

116. Программы для защиты детей в Интернете в Албании: перспективная практика, ЮНИСЕФ, 2020 г.
117. Закон о кибербезопасности 2020 г., Правительство Ганы, Министерство связи и цифровизации (Закон 1038), 2020 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >



< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

3 Персональные данные, идентичность и самостоятельность

> **Государства-участники должны принять законодательные, административные и другие меры для обеспечения уважения и защиты частной жизни детей всеми организациями и во всех условиях, где обрабатываются их данные. Законодательство должно предусматривать надежные гарантии, прозрачность, независимый надзор и доступ к средствам правовой защиты. Государства-участники должны требовать интеграции встроенного алгоритма конфиденциальности в цифровые продукты и услуги, ориентированные на детей. Они должны регулярно пересматривать законодательство о конфиденциальности и защите данных и с помощью процедур и практических методов обеспечивать предотвращение преднамеренных или случайных нарушений неприкосновенности частной жизни детей. в тех случаях, когда шифрование считается подходящим средством, государства-участники должны рассмотреть соответствующие меры, позволяющие обнаруживать и сообщать о сексуальной эксплуатации детей и жестоком обращении с ними или о материалах по сексуальными надругательствами над детьми. Такие меры должны строго ограничиваться в соответствии с принципами законности, необходимости и соразмерности.**
>
> Источник: Замечание общего порядка № 25 (2021 г.), п. 701[118]

Цель

Осознавать преимущества и реагировать на текущие и возникающие угрозы неприкосновенности конфиденциальности, личным данным и свободе действий детей в цифровом мире, связанные с использованием данных, включая персональные данные, технологию биометрической идентификации и систему автоматизированного принятия решений.

Текст типовой политики

Для обеспечения целостного подхода к безопасности детей в Интернете необходимо предпринять следующие шаги.

3a. Создать системы защиты данных или обеспечить эффективность действующих систем такого рода конкретно для защиты данных о детях
Права детей в Интернет-среде тесно связаны с тем, как собираются, хранятся и используются их данные. Законодательство и регулирование в области защиты данных для детей должны быть доступными, эффективными и способными к эволюции в соответствии с возникающими рисками.[119] Это означает не только разработку нормативно-правового регулирования, но и обеспечение его практической эффективности и внедрения.

3b. Установить протоколы и ограничения на использование систем автоматизированного принятия решений, которые могут повлиять на детей
Стандарты, законы, нормы и правила должны обеспечивать, чтобы дети могли пользоваться преимуществами автоматизированных систем и их права не ущемлялись вследствие автоматизированного принятия решений.[120] Особенно важно избегать потенциальной дискриминации вследствие автоматизированного принятия решений. Такие протоколы и ограничения могут применяться, в частности, в контексте уголовного правосудия, социального обеспечения, здравоохранения, медицины, образования и частного сектора. ▶

118. Замечание общего порядка № 25 (2021 г.) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка, 2021 г.
119. Общий регламент о защите данных, Европейский союз, 2018 г.
120. «Мир скатывается в антиутопию цифрового благоденствия», предупреждение эксперта ООН по правам человека, Управление Верховного комиссара Организации Объединенных Наций по правам человека, 2019 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

3 Персональные данные, идентичность и самостоятельность

3c. Обеспечить надлежащую нормативно-правовую защиту биометрических данных детей
Правительству и регулирующим органам следует разработать соответствующие нормативно-правовые протоколы и ограничения в отношении использования биометрических данных детей с учетом их прав, целевых ограничений и требований политики обеспечения безопасности детей в Интернете.

3d. Создать четкое руководство, законы и нормативные акты в отношении практики, которая может повлиять на свободу действий детей Создайте правовую базу, предотвращающую адресную рекламу и отслеживание детей в коммерческих целях на основе их персональных данных. Установите нормы использования рекомендательных систем и других автоматизированных процессов принятия решений или технологий, которые могут управлять поведением детей, формировать предпочтения и мнения, подрывать репутацию или ограничивать возможности экспериментирования.[121]

3e. Обеспечить эффективный надзор и контроль
Создайте органы и системы, способные собирать информацию, касающуюся безопасности детей в Интернете, и обеспечьте прозрачность и эффективное осуществление прав и защиты детей со стороны предприятий, правительства и других организаций.

3f. Создать механизмы для обеспечения прозрачности
Надзор должен осуществляться назначенным регуляторным органом, обладающим достаточными ресурсами, необходимым потенциалом и компетенцией для понимания используемых систем и их влияния на права детей. Надзорный орган должен также иметь доступ к независимым исследованиям и экспертным знаниям.

121. См., например, Иск об утечке данных в YouTube, «Макканн против Google», 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

3 Персональные данные, идентичность и самостоятельность

План мероприятий для достижения цели

A **Создать или обеспечить эффективность существующих механизмов защиты данных для обеспечения специальной защиты данных о детях**

Права детей в Интернете тесно связаны с тем, как собираются, хранятся и используются их данные. Законодательство и регулирование в области защиты данных для детей должны быть доступными, эффективными и способными к эволюции в соответствии с возникающими рисками.[122] Это означает не только разработку нормативно-правового регулирования, но и обеспечение его практической эффективности.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Обратить внимание на разработанный в Великобритании Нормы проектирования с учетом возраста[123], которые являются золотым стандартом защиты данных о детях (см. «Прочие справочные ресурсы 2»).
2. Рассмотреть Общий регламент о защите данных (GDPR)[124] как модель для создания более широкого правового регулирования или регулирования с положениями о правоприменении и ключевыми определениями.
3. Изучить необходимость создания специальных или отдельных стандартов, например, стандартов для использования данных в сфере образования и здравоохранения или хранения данных государственными органами.
4. Убедиться, что они учтены в вашем плане, как это предусмотрено в пункте «Нормативно-правое регулирование» раздела «Область применения политики». См. «Средства поддержки 1» (стр. 80).

122. Общий регламент о защите данных, Европейский союз, 2018 г.
123. Нормы проектирования с учетом возраста — краткий обзор, Управление Комиссара по вопросам информации Великобритании, 2020 г.
124. Общий регламент о защите данных, Европейский союз, 2018 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

3 Персональные данные, идентичность и самостоятельность

B **Установить протоколы и ограничения на использование автоматизированного процесса принятия решений, которые могут повлиять на детей**

Стандарты, законы, нормы и правила должны обеспечивать, чтобы дети могли пользоваться преимуществами автоматизированных систем и их права не ущемлялись вследствие автоматизированного принятия решений.[125] Особенно важно избегать потенциальной дискриминации. Такие протоколы и ограничения могут применяться, в частности, в контексте уголовного правосудия, социального обеспечения, здравоохранения, медицины, образования и частного сектора.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, ознакомьтесь с последними законодательными актами, нормативными документами и международными техническими стандартами по разработке, аудиту и надзору в области ИИ в других юрисдикциях или региональных или международных организациях, например, Закон об искусственном интеллекте в ЕС[126], и адаптируйте их для своей страны.

125. «Мир скатывается в антиутопию цифрового благоденствия», предупреждение эксперта ООН по правам человека, Управление Верховного комиссара Организации Объединенных Наций по правам человека, 2019 г.
126. Предложение по Регламенту Европейского парламента и Совета, устанавливающее согласованные правила по искусственному интеллекту (Закон об искусственном интеллекте) и вносящее изменения в некоторые законодательные акты Союза COM/2021/206, EUR-Lex, 2021; Глобальная политика ИИ, Организация экономического сотрудничества и развития, 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

3 Персональные данные, идентичность и самостоятельность

C Обеспечить надлежащую нормативно-правовую защиту биометрических данных детей

Правительству и регулирующим органам следует разработать соответствующие нормативно-правовые протоколы и ограничения в отношении использования биометрических данных детей с учетом их прав, целевых ограничений и требований политики обеспечения безопасности детей в Интернете.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Узнать, подпадают ли биометрические данные под действие других национальных законов или нормативных актов (например, законодательства о данных). Возможно, некоторые законы, в которых не упоминаются биометрические данные, могут быть истолкованы как включающие их:[127]

   A. В таком случае обеспечьте более эффективную защиту детей.

   B. В случае, если ничего этого нет, необходимо разработать положение о биометрических данных. Оно должно охватывать биометрические данные, на получение которых было дано согласие (например, разблокировка телефона) и в тех случаях, когда согласие не было дано или его использование не очевидно (например, распознавание лиц на входе в школу или идентификация по отпечатку пальца для получения школьного обеда).

127. См., например, Чили: детей просят предоставить биометрические данные для получения продовольственных пайков в школах, Privacy International, 2019.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

3 Персональные данные, идентичность и самостоятельность

D **Создать четкое руководство, законы и нормативные акты в отношении практики, которая может повлиять на свободу действий детей**

Создайте правовую базу, предотвращающую адресную рекламу и отслеживание детей в коммерческих целях на основе их персональных данных. Установите нормы использования рекомендательных систем и других автоматизированных процессов принятия решений или технологий, которые могут управлять поведением детей, формировать предпочтения и мнения, подрывать репутацию или ограничивать возможности экспериментирования.[128]

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, будет полезно узнать о последних изменениях в законодательстве о данных, а также о появлении в других юрисдикциях нормативных актов, обеспечивающих справедливое использование личных профилей или ограничивающих их чрезмерное использование. Например, Нормы проектирования с учетом возраста (Великобритания),[129] Общий регламент о защите данных (GDPR, ЕС)[130] или Закон о цифровых услугах (ЕС)[131] и Кодекс неэфирной рекламы и прямого и рекламного маркетинга (CAP Code, Великобритания).[132]

128. См., например, Иск об утечке данных в YouTube, «Макканн против Google», 2021 г.
129. Нормы проектирования с учетом возраста, Управление Комиссара по вопросам информации Великобритании, 2020 г.
130. Общий регламент о защите данных, Европейский союз, 2018 г.
131. Закон о цифровых услугах: обеспечение безопасной и подотчетной Интернет-среды, Европейская комиссия, 2019 г.
132. Кодекс неэфирной рекламы и прямого и рекламного маркетинга, CAP Code, Великобритания.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

3 Персональные данные, идентичность и самостоятельность

E **Обеспечить эффективный надзор и контроль**

Создать органы и системы, способные собирать информацию, касающуюся безопасности детей в Интернете, и обеспечьте прозрачность и эффективное осуществление прав и защиты детей со стороны предприятий, правительства и других организаций.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Обеспечить наличие учреждения или уполномоченного органа или органов, которые могут рекомендовать и применять согласованную практику. Например, руководящие принципы Национального центра по делам пропавших без вести и эксплуатируемых детей.[133]
2. Разъяснить это в стратегии, разработанной в пункте «Нормативно-правовое регулирование» раздела «Область применения политики» с указанием вертикали ответственности и надзора (стр. 56).

133. Наша работа, Национальный центр по делам пропавших и эксплуатируемых детей (NCMEC).

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

3 Персональные данные, идентичность и самостоятельность

F **Создать механизмы для обеспечения прозрачности**

Надзор должен осуществляться назначенным регулирующим органом, обладающим достаточными ресурсами, необходимым потенциалом и компетенцией для понимания используемых систем и их влияния на права детей. Надзорный орган должен также иметь доступ к независимым исследованиям и экспертным знаниям.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, убедитесь, что выбранный регулирующий орган предусмотрен законом, обеспечен ресурсами и наделен соответствующими полномочиями. Например, Управление Комиссара по вопросам информации.[134] Управление Комиссара по вопросам информации является независимым органом Великобритании, созданным для защиты информационных стандартов и прав в интересах общества. или Национальное управление по защите данных, действующее в соответствии с Общим законом Бразилии о защите данных.[135]

134. Управление Комиссара по информации Великобритании.
135. Национальное управление по защите данных, Федеральное правительство Бразилии.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

Как это согласуется с основополагающими документами

Принятие гарантий, связанных с цифровой идентификацией, имеет решающее значение для правительств и Организации Объединенных Наций в их стремлении полностью реализовать ее возможности и потенциал, а также укрепить доверие к ее использованию. Это включает, например, такие меры, как децентрализованное хранение данных, идентификация и аутентификация, зашифрованные коммуникации и рассмотрение возможности использования принципов встроенного алгоритма конфиденциальности.

Источник: План мероприятий Генерального секретаря ООН по цифровому сотрудничеству, июнь 2020 г.[136]

Если необходимо получение согласия на обработку данных ребенка, государства-участники должны обеспечить, чтобы согласие было информированным и получалось без принуждения от ребенка или, в зависимости от его возраста и развития, от родителя или опекуна до обработки этих данных. Если собственное согласие ребенка считается недостаточным и для обработки персональных данных ребенка требуется согласие родителей, государства-участники должны требовать, чтобы организации, обрабатывающие такие данные, проверяли, что согласие является информированным, осмысленным и было дано родителем или опекуном ребенка.

Источник: Замечание общего порядка № 25 (2021 г.), п. 71[137]

Государства-участники должны обеспечить, чтобы дети и их родители или опекуны могли легко получить доступ к сохраненным данным, исправить неточные или устаревшие данные и удалить данные, незаконно или без необходимости сохраненные государственными органами, частными лицами или другими органами, с учетом разумных и законных ограничений. Кроме того, они должны обеспечить право детей отзывать согласие и возражать против обработки персональных данных, если оператор персональных данных не демонстрирует законных и веских оснований для их обработки. Они также должны предоставлять детям, родителям и опекунам информацию по таким вопросам на понятном для детей языке и в доступной им форме.

Источник: Замечание общего порядка № 25 (2021 г.), п. 72[138]

136. План мероприятий Генерального секретаря Организации Объединенных Наций по цифровому сотрудничеству, Организация Объединенных Наций, июнь 2020 года.
137. Замечание общего порядка № 25 (2021 год) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.
138. Замечание общего порядка № 25 (2021 год) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

3 Персональные данные, идентичность и самостоятельность

Процесс a («Создать или обеспечить эффективность существующих механизмов защиты данных для обеспечения специальной защиты данных о детях») требует обеспечения надлежащей защиты всех аспектов данных о детях в законодательстве и нормативных актах. Этот инструмент предназначен для того, чтобы помочь законодателям осмыслить широкий круг вопросов, которые необходимо решать в рамках системы защиты данных в интересах детей.

Средства поддержки

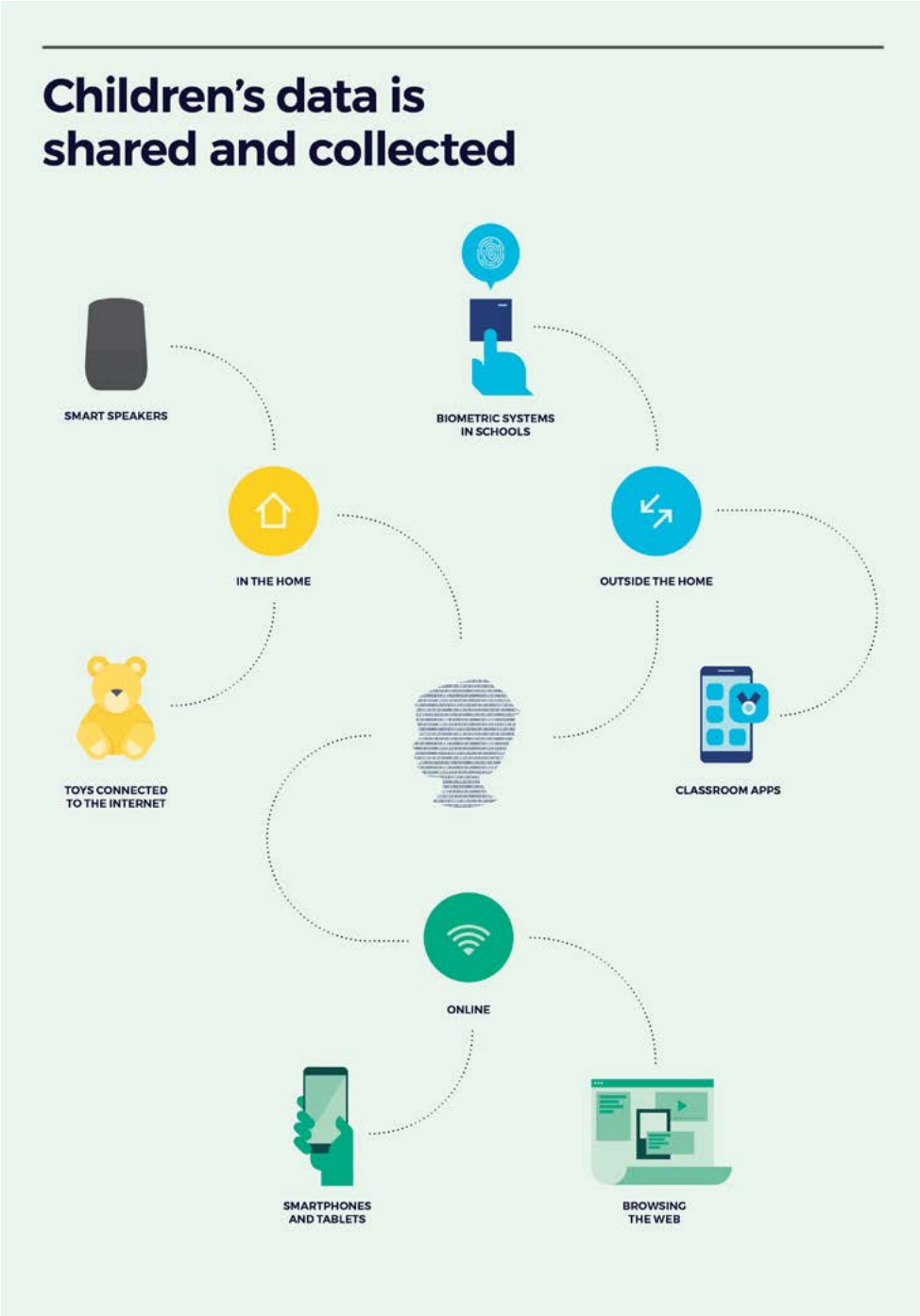
1. Контрольный список для создания всеобъемлющего законодательства о защите данных о детях

Есть ли у вас механизмы защиты данных, которые охватывают:	
Сбор	
Хранение	
Использование	
Данные об образовании	
Данные о здоровье	
Государственные и административные данные	
Данные, используемые для автоматизированного принятия решений	
Данные, используемые в других системах ИИ	
Биометрические данные	

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

Прочие справочные ресурсы

1. Визуальные материалы, помогающие понять широту и объем собранных данных о детях



Источник: Инфографика «Кто что знает обо мне», Уполномоченный по делам детей[139]

139. «Кто что знает обо мне», Уполномоченный по делам детей, 2018 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

3 Персональные данные, идентичность и самостоятельность

Источник: Инфографика «Кто что знает обо мне», Уполномоченный по делам детей[140]

2. Тематическое исследование британских Норм проектирования с учетом возраста[141]

В Великобритании был принят новаторский законодательный документ, касающийся использования данных о детях, под названием *«Нормы проектирования с учетом возраста»*.

> **«В этом документе рассматривается вопрос о том, как разработать гарантии защиты данных в Интернет-сервисах таким образом, чтобы они подходили для использования детьми и отвечали их потребностям в развитии. Он отражает растущую обеспокоенность положением детей в обществе и, в частности, в современном цифровом мире. На международном уровне и в Великобритании существует понимание того, что необходимо сделать гораздо больше для создания безопасного Интернет-пространства, в котором дети могли бы учиться, познавать и играть. Данный документ достигает этого не путем стремления защитить детей от цифрового мира, а путем их защиты внутри него».**

В документе изложены 15 стандартов проектирования с учетом возраста, отражающих подход, основанный на оценке рисков. Основное внимание уделяется настройкам по умолчанию, которые обеспечивают детям максимально удобный доступ к Интернет-сервисам при минимизации сбора и использования данных по умолчанию. Эти стандарты следующие:

1. Наилучшее обеспечение интересов ребенка
2. Оценки воздействия на защиту данных
3. Использование в соответствии с возрастом
4. Прозрачность
5. Использование данных во вред
6. Правила и нормы сообщества
7. Настройки по умолчанию
8. Минимизация использования данных
9. Обмен данными
10. Геолокация
11. Родительский контроль
12. Составление профиля
13. Методы побуждения
14. Сетевые игрушки и устройства
15. Онлайн-инструменты

140. «Кто что знает обо мне», Уполномоченный по делам детей, 2018 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

Нормы проектирования с учетом возраста вступили в силу в Великобритании 2 сентября 2021 года. Они основаны на Общем регламенте ЕС о защите данных (GDPR) и поэтому, вероятно, уже известны в странах, где соблюдаются требования GDPR. Широко распространено мнение о том, что это самый передовой режим защиты данных о детях в мире. После его принятия Интернет-сервисы объявили о целом ряде изменений в своем взаимодействии с детьми, включая следующие:

- В Instagram взрослые не могут направлять личные сообщения детям младше 18 лет, которые на них не подписаны.
- Безопасный поиск в Google будет включен по умолчанию для всех пользователей младше 18 лет.
- На YouTube автовоспроизведение отключено для детей младше 18 лет, а напоминания о перерывах и отходе ко сну включены по умолчанию.
- Дети младше 16 лет не могут вести прямые трансляции на TikTok, а после 21:00 у них отключаются push-уведомления.
- Google и Facebook отключат поведенческую рекламу для детей.

На конкретные сектора или типы информации могут распространяться дополнительные положения, например, данные о здоровье, финансовые данные и данные об образовании. Другие области также могут нуждаться в дополнительных нормах или дополнениях, но все они должны соответствовать высокому уровню конфиденциальности и отвечать интересам детей.

3. Манифест ЮНИСЕФ о совершенствовании управления данными о детях[142]

Рабочая группа ЮНИСЕФ по управлению данными подготовила отчет, в котором обоснована необходимость и изложены принципы улучшения управления данными о детях. Десять пунктов манифеста посвящены использованию данных в интересах детей, работе с самими детьми для понимания ими пользы использования данных, а также заполнению пробела в знаниях между технологиями и учреждениями и людьми, которые их используют.

4. Концепция конфиденциальности ОЭСР[143]

Концепция конфиденциальности ОЭСР объединяют ключевые компоненты концепции конфиденциальности ОЭСР, основанные на пересмотренных Руководящих принципах конфиденциальности:

ОСНОВНЫЕ ПРИНЦИПЫ НАЦИОНАЛЬНОГО ПРИМЕНЕНИЯ:

Принцип ограничения сбора данных
Сбор персональных данных должен быть ограничен, а любые такие данные должны быть получены законными и справедливыми средствами и, при необходимости, с ведома или согласия субъекта данных.

Принцип качества данных
Личные данные должны соответствовать целям, для которых они используются, и в той степени, в какой это необходимо для этих целей, должны быть точными, полными и актуальными.

141. Нормы проектирования с учетом возраста, Управление Комиссара по вопросам информации Великобритании, 2020 г.
142. За совершенствование управлением данными о детях: манифест, Бюро ЮНИСЕФ по глобальному анализу и политике, 2021 г.
143. Рекомендация Совета относительно руководящих принципов, регулирующих защиту частной жизни и трансграничный обмен персональными данными, Организация экономического сотрудничества и развития, 2013 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

Принцип определения цели
Цели, для которых собираются персональные данные, должны быть определены не позднее, чем в момент сбора данных, а последующее их использование ограничено выполнением данных целей или других, которые не являются несовместимыми с данными целями и которые определяются при каждом изменении цели.

Принцип ограничения использования данных
Персональные данные не должны раскрываться, предоставляться или иным образом использоваться для иных целей, помимо целей, определенных в параграфе 9. Однако раскрытие, предоставление и иное использование также возможно a) с согласия субъекта данных или b) на основании закона.

Принцип обеспечения безопасности
Личные данные должны быть защищены разумными мерами безопасности от таких рисков, как потеря или несанкционированный доступ, уничтожение, использование, изменение или раскрытие данных.

Принцип открытости
Следует проводить общую политику открытости в отношении разработок, практики и политики в отношении персональных данных. Должны быть доступны средства установления существования и характера персональных данных, основных целей их использования, а также личности и обычного места жительства оператора данных.

Принцип участия частных лиц
Каждый человек должен иметь право:

a) получить от оператора данных или иным образом подтверждение того, располагает ли оператор данными, относящимися к нему;

б) получить данные, относящиеся к нему

  i. в разумный срок;

  ii. за умеренную плату, если таковая предусмотрена;

  iii. приемлемым способом; и

  iv. в доступной для него форме;

c) получить разъяснения причин, если в просьбе, поданной в соответствии с подпунктами (a) и (b), отказано, и иметь возможность обжаловать такой отказ; и

d) оспорить относящиеся к нему данные и, в случае успешного для него разрешения спора, добиться их удаления, исправления, дополнения или изменения.

Принцип подотчетности
Оператор данных должен нести ответственность за соблюдение мер, обеспечивающих реализацию вышеизложенных принципов.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

Основные принципы международного применения: свободный обмен и законные ограничения

- Оператор данных несет ответственность за персональные данные, находящиеся в его распоряжении, независимо от местонахождения данных.
- Страна-член должна воздерживаться от ограничения трансграничного обмена персональными данными с другой страной, если (a) другая страна в значительной степени соблюдает настоящее Руководство или (b) существуют достаточные гарантии, включая эффективные механизмы правоприменения и соответствующие меры, принятые оператором данных, для обеспечения постоянного уровня защиты в соответствии с настоящим Руководством.
- Любые ограничения на трансграничные потоки персональных данных должны быть пропорциональны существующим рискам, с учетом конфиденциальности данных, а также цели и контекста их обработки.

5. **Общий регламент Европейского союза о защите данных (текст и инструменты)[144]**
Общий регламент о защите данных (GDPR) — это закон о конфиденциальности и безопасности, утвержденный Европейским союзом. Он требует от предприятий, работающих в европейских странах и за их пределами, правомерного использования персональных данных граждан ЕС.

6. **Европейская цифровая стратегия (включая предложения по искусственному интеллекту и данным)[145]**
Это руководство поможет понять, каким образом Европейский Союз создает свое цифровое будущее. Европейская цифровая стратегия направлена на развитие единого рынка, на котором все компании смогут конкурировать на равных условиях, не нарушая права потребителей на конфиденциальность, и на улучшение цифрового сообщества в регионе и во всем мире.

7. **Основы ориентированного на ребенка подхода к обработке данных (Основы), Ирландская комиссия по защите данных[146]**
Разработанные Ирландской комиссией по защите данных «Основы» направлены на улучшение стандартов обработки данных. Они служат руководством для организаций, занимающихся обработкой данных о детях, с учетом принципов, разработанных в соответствии с GDPR.

8. **Меморандум ЮНИСЕФ об искусственном интеллекте и правах детей[147]**
В меморандуме, подготовленном ЮНИСЕФ, изложены ключевые элементы того, как ИИ влияет на права детей в различных областях, таких как популярная видеоплатформа YouTube, интеллектуальные игрушки и ИИ в образовании. в нем также содержатся первоначальные рекомендации для законодателей, корпораций, родителей и работников сферы образования.

9. **Под наблюдением: биометрические данные. Системы ИТ и основные права в ЕС, отчет Агентства Европейского Союза по основным правам[148]**
Системы информационных технологий (ИТ), разработанные ЕС, играют жизненно важную роль в обеспечении региональной безопасности, например, в регулировании миграции и борьбе с терроризмом и серьезными преступлениями. Однако влияние этих систем на основные права человека еще предстоит изучить. Например, с учетом положений статьи 24 Конвенции УВКПЧ о правах ребенка, доклад в главе 7 подчеркивает, что при сборе данных биометрической идентификации системы должны в первую очередь учитывать интересы ребенка.

144. Общий регламент о защите данных, Европейский союз, 2018 г.
145. Создание цифрового будущего Европы, Европейский Союз, 2020 г.
146. Основы ориентированного на ребенка подхода к обработке данных, Ирландская комиссия по защите данных, 2020 г.
147. Искусственный интеллект и права детей, Детский фонд Организации Объединенных Наций, 2019 г.
148. Под наблюдением: биометрические данные. Системы ИТ и основные права в ЕС, Агентство по основным правам, ЕС, 2018 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

10. Руководство ЮНИСЕФ по вопросам искусственного интеллекта для детей[149]
Хотя системы ИИ широко внедряются странами, обеспокоенность по поводу этой новой технологии также побудила правительства, компании и гражданское общество разработать принципы ее этического использования. Хотя права человека были включены в эти стратегии ИИ, правам детей, в частности, пока что не уделяется достаточно внимания. в этом руководстве ЮНИСЕФ стремится повысить осведомленность о правах детей и дать рекомендации различным сторонам, в основном законодателям и представителям деловых кругов, в отношении политики и практики в области ИИ в применении к детям.

Голосовые помощники и чат-боты на базе ИИ

Виртуальные голосовые помощники и чат-боты используют обработку языковой информации (NLP, Natural Language Processing), автоматическое распознавание речи и машинное обучение для распознавания словесных команд, выявления закономерностей, получения информации и выдачи ответов. Хотя не все эти системы созданы или приспособлены для детей, миллионы детей попадают под их влияние в эмоциональном или поведенческом плане. Сторонники этих технологий называют среди их преимуществ поддержку детей с нарушениями зрения или ограниченной подвижностью, а также новые способы обучения и стимулирования детского любопытства и творчества. Кроме того, некоторые чат-боты призваны облегчить учебу и сэкономить время учащихся.

Однако использование чат-ботов чревато дополнительными рисками для детей, особенно в сфере психического здоровья, когда боты не распознают призывы о помощи или дают неправильные советы. Например, в ходе тестирования двух чат-ботов, посвященных психическому здоровью, проведенного BBC в 2018 году, выяснилось, что приложения не смогли должным образом обработать сообщения детей о сексуальном насилии, хотя оба приложения были признаны подходящими для детей. Согласно докладу ЮНИСЕФ, «при непродуманной разработке чат-боты могут создавать, а не решать проблемы», что «особенно опасно в случае молодых пользователей, которые могут оказаться недостаточно эмоционально устойчивыми, чтобы справиться с негативным или непонятным опытом общения с чат-ботом». Более того, чат-боты могут создавать различные угрозы безопасности, включая спуфинг (попытку выдать себя за другого человека), подделку данных, кражу данных и уязвимость к кибератакам, а также могут навязывать предвзятость, поскольку часто выбирают заранее определенный ответ на основе наиболее подходящих ключевых слов или похожих формулировок.

Другие проблемы, связанные с технологиями чат-ботов и персональных помощников, связаны с конфиденциальностью и правами собственности на данные. Например, учитывая, что голосовым помощникам обычно нужно сохранять голосовые записи для облегчения непрерывного обучения системы, защитники прав ребенка поднимают вопрос об отсутствии ясности в политике хранения данных компанией и согласия на это детей и родителей.

Распознавание лиц для биометрической идентификации

Системы распознавания лиц используют методы компьютерного зрения и алгоритмы машинного обучения для определения, обработки и анализа черт лица человека с широким спектром целей, таких как сверка личности человека с существующей записью. в целях идентификации она может использоваться для пограничного контроля, анализа и предотвращения преступлений, а также в школьных системах видеонаблюдения по соображениям повышенной безопасности. Распознавание лиц все чаще используется в качестве цифрового «удостоверения» личности как для юридической, так и для функциональной идентификации. Хотя эта технология не заменяет юридическое удостоверение личности, которое делает человека видимым для государства и является признанным правом, она может быстрее и проще подтвердить существующую идентификационную запись.

149. Руководство по созданию политики в области искусственного интеллекта для детей, Детский фонд Организации Объединенных Наций, 2020 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

Связанные с этим риски и ограничения в области прав человека и прав ребенка велики. Защитники конфиденциальности предостерегают против его реального использования в рамках государственных мероприятий по массовой слежке в качестве инструмента расследования правоохранительных органов, особенно в связи с тем, что он может быть использован для профилирования, отслеживания и подавления уязвимых сообществ. в некоторых случаях эти системы также поднимают вопрос об осмысленном согласии, поскольку люди могут не знать о том, кто собирает их биометрические данные или даже о том, что они собираются, как хранятся или как могут быть использованы. Кроме того, по-прежнему наблюдаются неточности в распознавании лиц, включая менее надежное сопоставление лиц детей и других групп в зависимости от пола и этнической принадлежности, например, цветных женщин. Как следствие, это может закрепить существующие социальные предубеждения и привести к дискриминации или дальнейшей маргинализации меньшинств.

Источник: Руководство по созданию политики в области искусственного интеллекта для детей, Детский фонд Организации Объединенных Наций, 2020 г.[150]

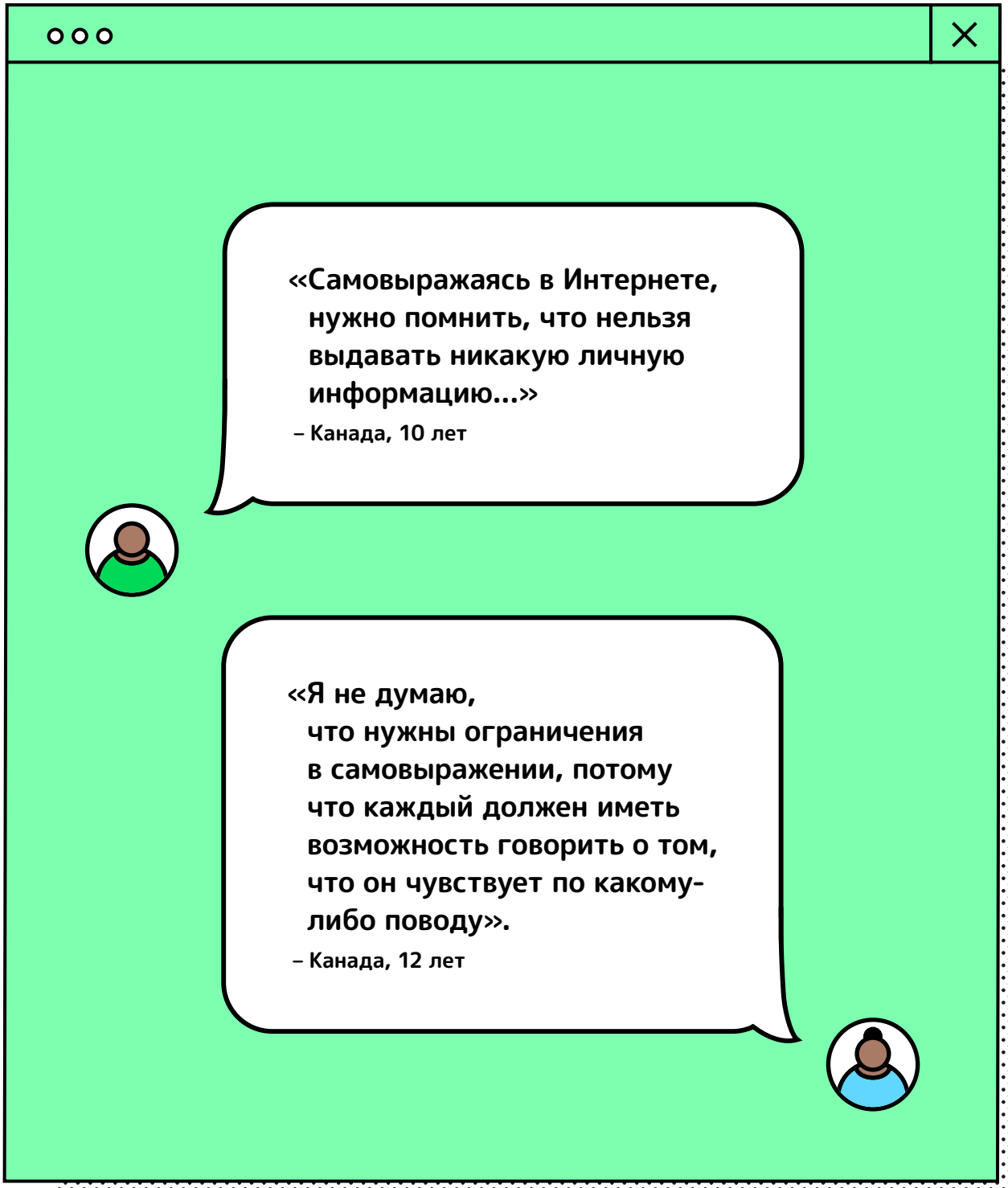
1. **Законодательство о детях: дополнительные ресурсы[151]**
   На этом сайте размещены все дополнительные ресурсы Управления Комиссара по информации Великобритании о Нормах проектирования с учетом возраста, включая часто задаваемые вопросы и Шаблон оценки воздействия на защиту данных.

2. **Демистификация Норм проектирования с учетом возраста, Фонд 5Rights[152]**
   Это брошюра для детей о разработке британских Норм проектирования с учетом возраста.

150. Руководство по созданию политики в области искусственного интеллекта для детей, Детский фонд Организации Объединенных Наций, 2020 г.
151. Законодательство о детях: дополнительные ресурсы, Управление Комиссара по вопросам информации, 2021 г.
152. Демистификация Норм проектирования с учетом возраста, Фонд 5Rights, 2020 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >



< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

4 Системы реагирования и поддержки

Государства-участники должны предоставлять детям информацию с учетом их интересов и возраста на понятном для детей языке об их правах и о механизмах подачи и рассмотрения жалоб, услугах и средствах правовой защиты, доступных им в случае нарушения или злоупотребления их правами применительно к цифровой среде. Такая информация должна также предоставляться родителям, опекунам и специалистам, работающим с детьми и в их интересах.

Источник: Замечание общего порядка № 25 (2021 г.), п. 49[153]

Механизм 4 Модели национального реагирования. Надлежащая практика правоохранительной деятельности

В странах, в настоящее время не имеющих специального правоохранительного механизма по борьбе с сексуальной эксплуатацией детей и жестоким обращением с ними (CSEA), национальное правоохранительное ведомство должно разработать и взять на себя обязательства по созданию такого механизма.

В странах, уже имеющих специальный правоохранительный механизм по борьбе с CSEA, но все еще нуждаются в разработке многостороннего подхода, привлечение узких специалистов по защите детей к работе вместе со следователями является важным первым шагом. При планировании и проведении расследования случаев CSEA следует всегда руководствоваться принципами защиты детей в правоохранительной деятельности; это обеспечит приоритетность потребностей и прав ребенка. Многосторонний подход обеспечит более высокий уровень защиты и поддержки жертвы и поможет получить от нее наилучшие доказательства, что повысит вероятность успешного судебного преследования. Желательно также наладить обмен передовым опытом в регионе.

Источник: Модель национального реагирования Глобального альянса WeProtect[154]

Цель

Создать скоординированную многостороннюю структуру для борьбы с рисками для детей в Интернете, в частности, с сексуальной эксплуатацией детей и жестоким обращением с ними (CSEA), включая эффективные механизмы правового и нормативного обеспечения, предотвращения, средства правовой защиты и доступ к консультациям с экспертами по вопросам безопасности детей в Интернете.

153. Замечание общего порядка № 25 (2021 г.) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.
154. Под сексуальной эксплуатацией детей и жестоким обращением с ними (CSEA) подразумеваются случаи, когда ребенка принуждают или убеждают принять участие в сексуальных действиях. Речь может идти о физическом контакте или бесконтактных действиях, и такие действия могут происходить в Интернете или за его пределами.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

4 Системы реагирования и поддержки

Текст типовой политики

Для обеспечения целостного подхода к безопасности детей в Интернете необходимо предпринять следующие шаги.

4a. Уведомление о контенте и его удаление
Государственные учреждения должны сотрудничать с экспертами, правоохранительными органами и представителями отрасли в целях создания и мониторинга эффективных протоколов уведомления о незаконных и вредных материалах, а также их удаления. Среди прочего, это потребует разработки протоколов и законодательства, позволяющего местным интернет-провайдерам ограничивать доступ к хостам, которые не удаляют подозрительный контент или постоянно нарушают законы или другие нормативные требования в отношении безопасности детей в Интернете.

4b. Установить процессы управления рисками для правонарушений в сфере сексуальной эксплуатации детей и жестокого обращения с ними (CSEA)
Необходимо наладить эффективный многосторонний процесс управления правонарушителями, опираясь на международные стандарты надлежащей практики. Правоохранители и другие работники системы уголовного правосудия должны пройти подготовку по выявлению и расследованию противоправного поведения. Управление рисками нарушителей в этой сфере является важным компонентом концепции безопасности детей в Интернете, поскольку от отдельных лиц или групп правонарушителей в Интернете может пострадать большое число детей.

4c. Предоставить достаточное количество ресурсов для оказания психосоциальной поддержки детям, ставшим непосредственными и косвенными жертвами преступлений, и членам их семей
Организации, обучающие специалистов в области психического здоровья, психологии и социальной работы, которые работают с уязвимыми детьми, должны иметь базовое представление о вопросах безопасности детей в Интернете.[155] Безопасность детей в Интернете должна быть интегрирована в более широкие системы безопасности и защиты детей, такие как безопасность в школах или насилие в отношении детей (VAC).

4d. Создать механизмы выявления и защиты жертв
Одной из ключевых целей в деле предотвращения вреда, причиняемого в Интернете, является учет потребностей уязвимых детей и оптимальных способов их поддержки. Центры «одного окна» выступают в качестве первоначального комплексного учреждения для жертв насилия, обеспечивая доступ к целому ряду основных услуг — от медицинской до юридической помощи — из одного места. Такие центры закладывают основу для процедур защиты детей, оказывают поддержку жертвам и оперативно передают сообщения о преступлениях, совершаемых в Интернете, соответствующим органам.[156]

4e. Создать механизмы, не криминализирующие детей
Важно создать надлежащие механизмы для работы с детьми, нарушившими законы, связанные с безопасностью детей в Интернете, например в случаях кибербуллинга, распространения вредоносной информации или взлома. Дети должны быть по возможности исключены из системы уголовного судопроизводства. Следует отдавать предпочтение возможностям консультирования или восстановительного правосудия. Важно также убедиться, что в расчет принимаются все обстоятельства ребенка. Например, поведение ребенка может быть результатом буллинга, домогательств или иной формы принуждения.

155. Эффективные методы предотвращения насилия против женщин и девочек: обзор доказательств, статья 3 «Механизмы реагирования для предупреждения насилия», What Works, 2015 г. стр. 28.
156. Предотвращение сексуальной эксплуатации детей и жестокого обращение с ними (CSEA): Модель национального реагирования, Глобальный альянс WeProtect, 2016 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

4 Системы реагирования и поддержки

План мероприятий для достижения цели

A Уведомление о контенте и его удаление

Государственные учреждения должны сотрудничать с экспертами, правоохранительными органами и представителями отрасли в целях создания и мониторинга эффективных протоколов уведомления о незаконных и вредных материалах, а также их удаления. Среди прочего, это потребует разработки протоколов и законодательства, позволяющего местным интернет-провайдерам ограничивать доступ к хостам, которые не удаляют подозрительный контент или постоянно нарушают законы или другие нормативные требования в отношении безопасности детей в Интернете.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Разработать и реализовать планы по устранению пробелов в законодательстве. См. «Средства поддержки 1» (стр. 97).
2. В качестве руководства используйте основополагающие документы, представленные в Ключевых документах, и другие ресурсы, в частности, Модель национального реагирования (MNR)[157] (см. «Прочие справочные ресурсы 1»).

157. Предотвращение сексуальной эксплуатации детей и жестокого обращение с ними (CSEA): Модель национального реагирования, Глобальный альянс WeProtect, 2016 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

4 Системы реагирования и поддержки

B **Установить процессы управления рисками для правонарушений в сфере сексуальной эксплуатации детей и жестокого обращения с ними (CSEA)**

Необходимо наладить эффективный многосторонний процесс управления правонарушителями, опираясь на международные стандарты надлежащей практики. Правоохранители и другие работники системы уголовного правосудия должны пройти подготовку по выявлению и расследованию противоправного поведения. Управление рисками правонарушителей является важным компонентом концепции безопасности детей в Интернете, поскольку от отдельных лиц или групп правонарушителей в Интернете может пострадать большое число детей.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Обобщить имеющийся опыт, например, Национального агентства по борьбе с преступностью[158] и Европола, для создания богатой базы знаний.[159]
2. При необходимости обратиться за поддержкой к международным или региональным экспертам, таким как Национальный центр по проблемам пропавших и подвергающихся эксплуатации детей,[160] Фонд Internet Watch Foundation,[161] Интерпол[162] и ECPAT.[163]

158. О нас, Национальное агентство по борьбе с преступностью.
159. О Европоле, Европол.
160. Наша работа, Национальный центр по проблемам пропавших и подвергающихся эксплуатации детей.
161. О нас, Internet Watch Foundation (IWF).
162. Кто мы, ИНТЕРПОЛ.
163. Универсальная терминология: Терминологическое руководство по защите детей от сексуальной эксплуатации и сексуального насилия, ECPAT International, 2016 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

4 Системы реагирования и поддержки

C **Предоставить достаточное количество ресурсов для оказания психосоциальной поддержки детям, ставшим непосредственными и косвенными жертвами преступлений, и членам их семьей**

Организации, обучающие специалистов в области психического здоровья, психологии и социальной работы, которые работают с уязвимыми детьми, должны иметь базовое представление о вопросах безопасности детей в Интернете.[164] Безопасность детей в Интернете должна быть интегрирована в более широкие системы безопасности и защиты детей.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Включить долгосрочное развитие потенциала в области сексуальной эксплуатации и насилия над детьми в ваш текущий план. См. Средства поддержки 1 в пункте «Обучение» раздела «Область применения политики» для определения необходимых потребностей в обучении для наращивания потенциала (стр. 119).Ср
2. При необходимости обратиться за поддержкой к международным или региональным экспертам, таким как Национальный центр по проблемам пропавших и подвергающихся эксплуатации детей,[165] Фонд Internet Watch Foundation,[166] Интерпол[167] и ECPAT.[168]

164. Под сексуальным насилием над детьми (CSA) подразумеваются случаи, когда ребенка принуждают или убеждают принять участие в сексуальных действиях. Речь может идти о физическом контакте или бесконтактных действиях и может происходить в Интернете или в реальной жизни.
165. Наша работа, Национальный центр по проблемам пропавших и подвергающихся эксплуатации детей.
166. О нас, Internet Watch Foundation (IWF).
167. Кто мы, ИНТЕРПОЛ.
168. Универсальная терминология: Терминологическое руководство по защите детей от сексуальной эксплуатации и сексуального насилия, CPAT International, 2016 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

4 Системы реагирования и поддержки

D **Создать механизмы выявления и защиты жертв**

Одной из ключевых целей в деле предотвращения вреда, причиняемого в Интернете, является учет потребностей уязвимых детей и оптимальных способов их поддержки. Должны быть усилены возможности центров «единого окна» для обеспечения безопасности и защиты детей, оказания поддержки жертвам и быстрой передачи сообщений о преступлениях в Интернете в соответствующие органы.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Изучить существующие центры обслуживания по принципу «единого окна» (см., например, Модель национального реагирования (MNR)[169] в разделе «Прочие справочные ресурсы 1»). Например, полиция Шотландии.[170]
2. Для создания сети необходимых специалистов при необходимости обратитесь за поддержкой к международным или региональным экспертам, таким как Национальный центр по проблемам пропавших и подвергающихся эксплуатации детей,[171] Фонд Internet Watch Foundation,[172] Интерпол[173] и ECPAT.[174]

169. Предотвращение сексуальной эксплуатации детей и жестокого обращение с ними (CSEA): Модель национального реагирования, WeProtect, 2016 г.
170. Безопасность в Интернете, полиция Шотландии.
171. Наша работа, Национальный центр по делам пропавших и эксплуатируемых детей (NCMEC).
172. О нас, Internet Watch Foundation (IWF).
173. Кто мы, ИНТЕРПОЛ.
174. Универсальная терминология: Терминологическое руководство по защите детей от сексуальной эксплуатации и сексуального насилия, ECPAT International, 2016 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

4 Системы реагирования и поддержки

E **Создать механизмы, не криминализирующие детей**

Важно создать надлежащие механизмы для работы с детьми, нарушившими законы, связанные с безопасностью детей в Интернете, например в случаях кибербуллинга, распространения вредоносной информации или взлома. По возможности, дети должны быть выведены за пределы системы уголовного правосудия, при этом предпочтение следует отдавать возможностям психологической помощи или восстановительного правосудия. Важно также убедиться, что в расчет принимаются все обстоятельства ребенка. Поведение ребенка может быть результатом буллинга, домогательств или иной формы принуждения.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Привлечь ваше министерство юстиции к формулированию существующего закона (законов).
2. Провести консультации с ключевыми заинтересованными сторонами, включая детей, молодых людей и родителей/опекунов, чтобы при необходимости внести изменения или дополнения в законы и нормативные руководства.
3. Привлечь специалистов по правам ребенка, чтобы обеспечить реабилитацию и защиту несовершеннолетних, а не их наказание (за исключением самых серьезных случаев).

Как это согласуется с основополагающими документами

В странах, в настоящее время не имеющих специального правоохранительного механизма по борьбе с CSEA, национальное правоохранительное ведомство должно разработать и взять на себя обязательства по созданию такого механизма. Это включает назначение профильных сотрудников, которые будут занимать свои должности в течение минимального срока (предположительно не менее двух лет); выделение соответствующего помещения для размещения таких сотрудников; приобретение необходимого оборудования; предоставление специализированных курсов и методик в области CSEA; оказание психологической поддержки сотрудникам; разработка и проведение тренингов по повышению осведомленности о CSEA для местных правоохранительных органов по всей стране. в странах, уже имеющих специальный правоохранительный механизм по борьбе с CSEA, но все еще нуждаются в разработке многостороннего подхода, привлечение узких специалистов по защите детей к работе вместе со следователями является важным первым шагом. При планировании и проведении расследования случаев CSEA следует всегда руководствоваться принципами защиты детей в правоохранительной деятельности; это обеспечит приоритетность потребностей и прав ребенка. Многосторонний подход обеспечит более высокий уровень защиты и поддержки жертвы и поможет получить от нее наилучшие доказательства, что повысит вероятность успешного судебного преследования. Желательно также наладить обмен передовым опытом в регионе.

Источник: Модель национального реагирования Глобального альянса WeProtect[175]

175. Предотвращение сексуальной эксплуатации детей и жестокого обращение с ними (CSEA): Модель национального реагирования, Глобальный альянс WeProtect, 2016 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

Средства поддержки

1. Контрольный список для разработки надлежащих процедур уведомления о контенте и его удаления

Процесс А («Уведомление о контенте и его удаление») начинается с выявления пробелов в системах уведомления и удаления. Данный контрольный список предназначен для оказания помощи законодателям в определении шагов и требований, необходимых для обеспечения быстрого удаления незаконного и вредного контента после его обнаружения.

	Сформулировано юридическое определение незаконного контента	**Сформулированы правовые требования к удалению незаконного контента**	**Установлены временные рамки для удаления незаконного контента («уведомления об удалении»)**	**Сформулировано юридическое определение вредного, но не являющегося незаконным контента**	**Сформулированы правовые требования к удалению вредного контента**	**Установлены временные рамки для удаления вредного контента («уведомления об удалении»)**
Поставщики услуг Интернета						
Социальные сети						
Потоковые платформы						
Услуги облачного и иного хостинга						
Другое						

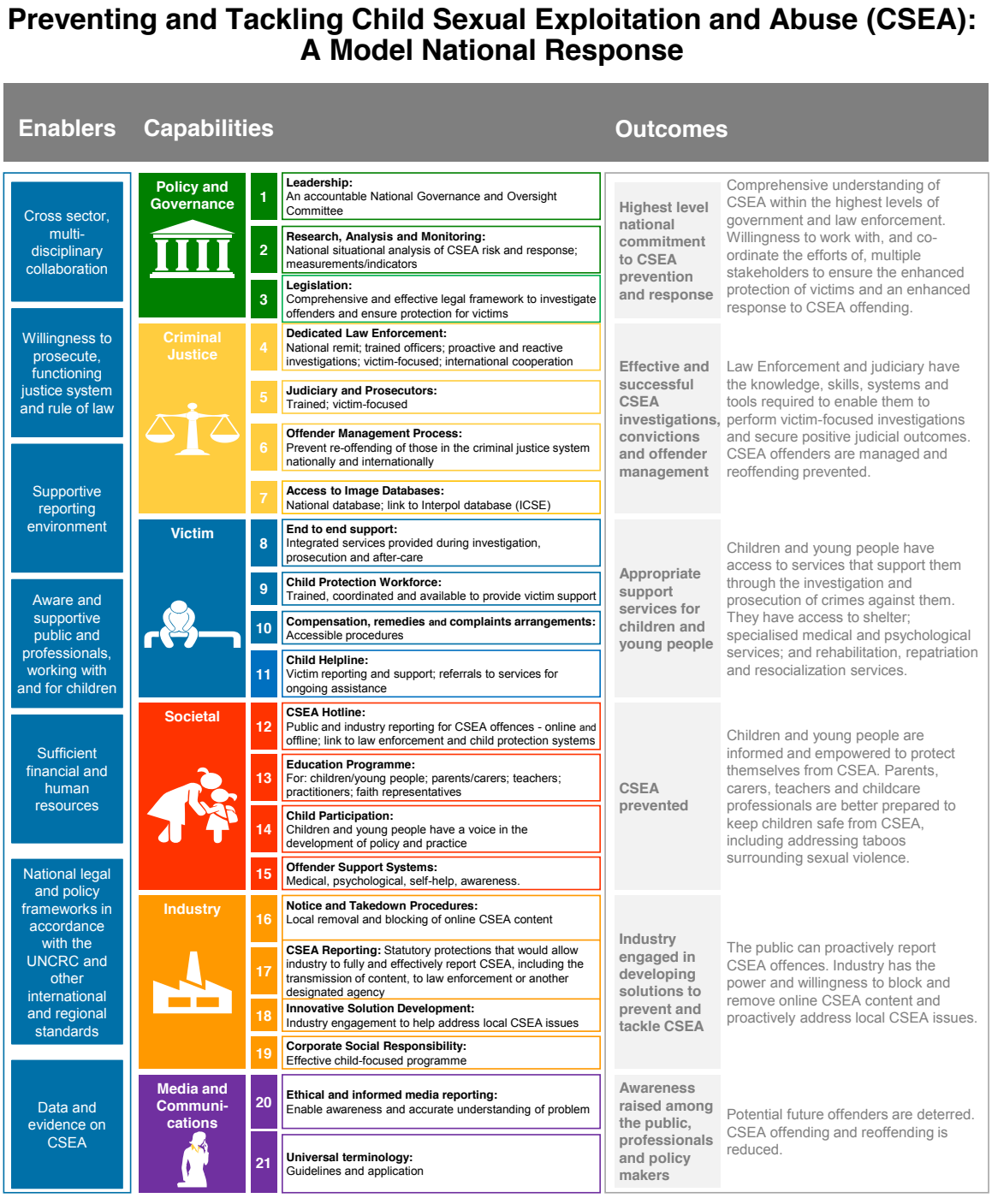
< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

4 Системы реагирования и поддержки

Прочие справочные ресурсы

1. Рабочие примеры Модели национального реагирования Глобального альянса WeProtect[176]



176. Рабочие примеры возможностей и реализации Модели национального реагирования, WeProtect, 2018 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

2. Австралийский законопроект о Законе о безопасности в Интернете[177]

Австралийский Закон о безопасности в Интернете включает:

- Обновление предыдущего австралийского законодательства, которое успешно работает (в частности, *Закона о повышении безопасности в Интернете 2015 года* и его схемы злоупотреблений с использованием изображений).
- Набор основных базовых ожиданий в отношении безопасности в Интернете для социальных сетей, соответствующих электронных сервисов и отдельных интернет-услуг, четко формулирующий ожидания сообщества и излагающий требования к обязательной отчетности.
- Расширенную схема борьбы с кибербуллингом для австралийских детей, охватывающую целый ряд Интернет-сервисов, а не только платформы социальных сетей.
- Новую схему борьбы с кибер-насилием для взрослых австралийцев для более эффективного устранения серьезных злоупотреблений и домогательств в Интернете.
- Модернизированную схему интерактивного контента, которая заменит схемы в Приложениях 5 и 7 Закона о вещательных службах 1992 года. Данный законопроект создаст новые классы опасного интерактивного контента и обновит устаревшие отраслевые кодексы для борьбы с таким контентом.
- Новые механизмы блокировки оскорбительных/насильственных материалов, которые позволят Комиссару по электронной безопасности быстро реагировать на кризисные события в Интернете, такие как террористические атаки в Крайстчерче, путем обращения к интернет-провайдерам с просьбой блокировать доступ к сайтам, содержащим серьезно опасный контент.
- Последовательные требования по удалению злоупотреблений с использованием изображений, киберагрессии, кибербуллинга и опасного онлайн-контента, обязывающие интернет-провайдеров удалять такие материалы в течение 24 часов после получения уведомления от Комиссара по электронной безопасности.

3. Инструменты проекта EndOCSEA@Europe[178]

Проект EndOCSEA (Противодействие сексуальной эксплуатации детей и жестокому обращению с ними в Интернете) был разработан для обеспечения защиты прав детей с помощью эффективного многонационального, междисциплинарного и межсекторального сотрудничества и ориентированных на детей мер по предотвращению и противодействию сексуальной эксплуатации детей и жестокому обращению с ними в Интернете (OCSEA) с использованием ИКТ на общеевропейском уровне.

Проект включает три взаимодополняющих компонента, каждый из которых направлен на:

- создание благоприятных условий для межсекторального, междисциплинарного сотрудничества на национальном и региональном уровнях путем укрепления национальных структур управления и проведения ситуационного анализа рисков OCSEA и мер реагирования в национальном и общеевропейском контекстах;
- поддержку законодательных и процедурных реформ, обучение и повышение компетенции сотрудников правоохранительных органов, судебной системы и прокуратуры, а также содействие междисциплинарному межведомственному сотрудничеству для оказания всесторонней поддержки жертвам; и
- решение социальных проблем с акцентом на повышение осведомленности, просвещение основных целевых групп и расширение прав и возможностей детей.

177. Консультации по законопроекту о новом Законе о безопасности в Интернете, Министерство инфраструктуры, транспорта, регионального развития и коммуникаций, 2020 г.
178. Противодействие сексуальной эксплуатации детей и жестокому обращению с ними в Интернете, Совет Европы, 2020 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

4. **Конвенция Совета Европы о киберпреступности (Будапештская конвенция)**[179]
   Это соглашение ЕС в отношении преступлений, совершаемых в Интернете и других компьютерных сетях и касающихся, в частности, нарушения авторских прав, компьютерного мошенничества, материалов по сексуальным надругательствам над детьми и нарушений сетевой безопасности. Конвенция также предусматривает ряд полномочий и процедур, таких как розыск в компьютерных сетях и перехват трафика.

5. **Руководство по работе горячей линии INHOPE**[180]
   Миссия INHOPE заключается в поддержке сети горячих линий по борьбе с материалами по сексуальным надругательствам над детьми в Интернете (CSAM). Ассоциация INHOPE включает множество горячих линий по всему миру, которые работают во всех странах-членах ЕС, России, Южной Африке, Северной и Южной Америке, Азии, Австралии и Новой Зеландии. Ассоциация INHOPE поддерживает горячие линии и их партнерские организации посредством обучения, передачи передового опыта, обеспечения качества и обеспечения персонала.

6. **Ресурсы ЮНИСЕФ и ассоциации GSMA об уведомлении о контенте и его удалении**[181]
   Это руководство для поставщиков интернет-услуг по политике и процедурам в отношении уведомления о контенте и его удалении, направленное на предотвращение неправомерного использования их услуг для обмена материалами по сексуальным надругательствам над детьми.

7. **R;pple Suicide Prevention**[182]
   R;pple Suicide Prevention — это инструмент онлайн-мониторинга для предотвращения самоубийств, который отображает специальную страницу на устройстве пользователя, как только будет замечено, что он ищет вредное ключевое слово или фразу, указанную в конфигурации инструмента мониторинга R;pple. Ключевые слова и фразы включают любые слова или термины, которые были определены как ссылки на потенциально вредный Интернет-контент.

8. **Тематическое исследование подхода Албании к оказанию помощи пострадавшим**[183]
   В данном исследовании хорошо представлена концепция сквозной поддержки. Она включает процедуру немедленного психосоциального консультирования детей, сообщивших о насилии в Интернете на Албанскую национальную линию помощи детям, ALO 116 111, и процедуру направления в соответствующие органы, так что в 2019 году все дети, сообщившие о насилии, при необходимости были направлены в соответствующие органы. Благодаря обширным инвестициям в укрепление потенциала сотрудников системы социального обеспечения была введена пересмотренная учебная программа по социальной работе, а в постоянную программу обучения без отрыва от работы Албанской школы государственного управления были включены вопросы уведомления и реагирования в случаях насилия в отношении детей в Интернете.

9. **Национальный план действий по предотвращению сексуальной эксплуатации детей в Интернете и реагированию на нее в Камбодже на 2021–2025 годы**[184]
   Этот план был разработан Технической рабочей группой по сексуальной эксплуатации детей в Интернете, в которую входят 11 правительственных министерств, ЮНИСЕФ и различные НПО. Признавая взаимосвязь между сексуальной эксплуатацией детей и жестоким обращением с ними в Интернете и в реальной жизни, данный план действий включен в более широкие рамки Плана действий по предотвращению насилия в отношении детей и реагированию на него на 2017-2021 годы, а также следующего этапа, начинающегося в 2022 году.

179. Будапештская конвенция, Совет Европы, 2021 г.
180. Наша история, INHOPE, 2021 г.
181. Политика и практика компаний по удалению материалов по сексуальным надругательствам над детьми в Интернете, Детский фонд ООН и GSMA, 2016 г.
182. R;pple Suicide Prevention, R;pple, 2021 г.
183. Программа защиты детей в Интернете в Албании: Перспективная практика, Детский фонд ООН, 2020 г.
184. Официальная презентация Национального плана действий по предотвращению сексуальной эксплуатацию детей в Интернете и реагированию на нее в Камбодже на 2021–2025 годы.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

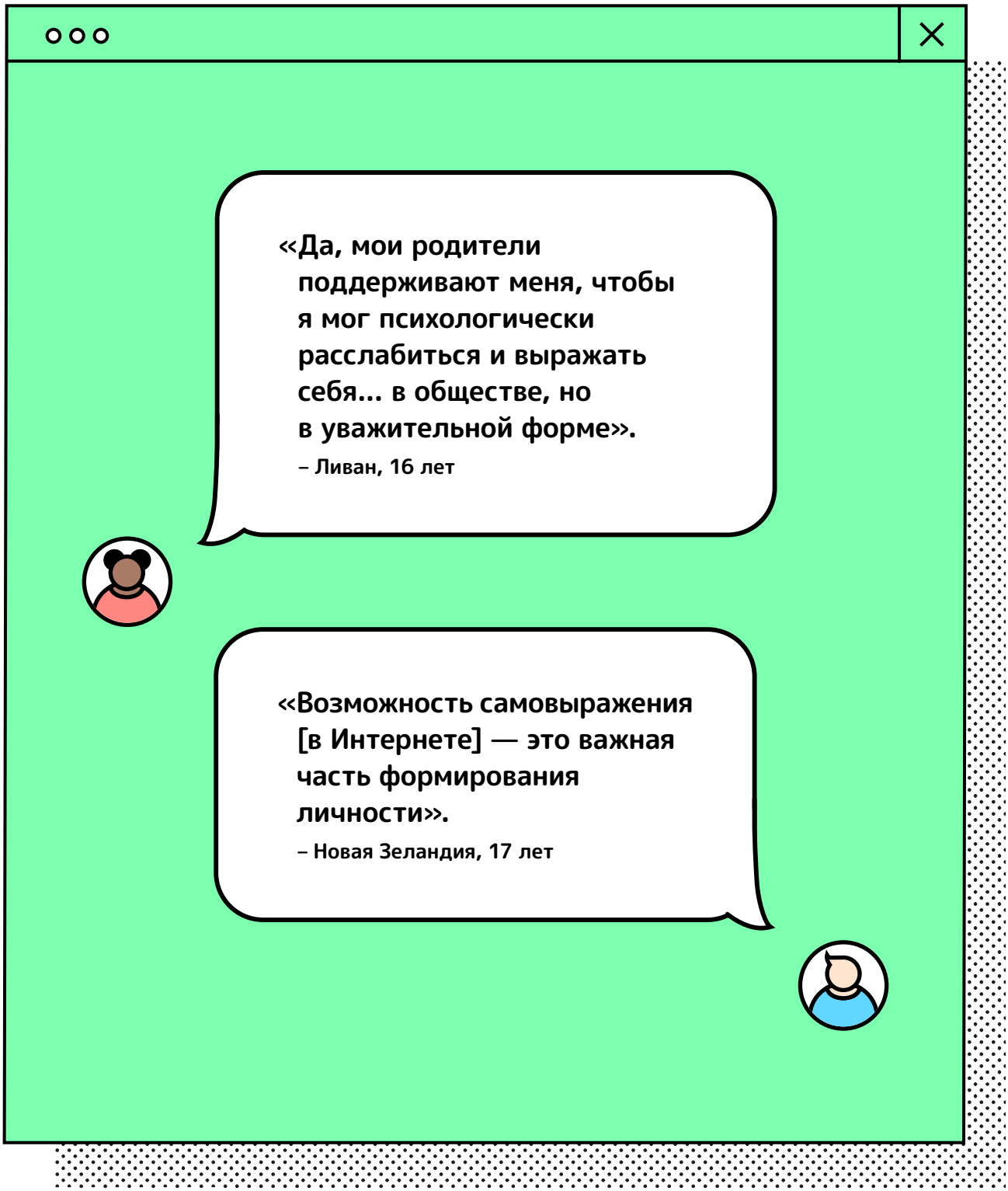
10. **Internet Watch Foundation (IWF)**[185]
    Фонд IWF занимается поиском, удалением, пресечением и предотвращением появления изображений сексуального насилия над детьми в Интернете. Он использует собственные уникальные, достоверные данные для исследования новых тенденций, тактик и методов, применяемых злоумышленниками в Интернете. Он использует эти компетенции для разработки передовых услуг, предназначенных для того, чтобы помочь технологическому сообществу предотвращать и пресекать появление изображения сексуального насилия над детьми в Интернете и удалять их по всему миру.

11. **Отдел Интерпола по борьбе с преступлениями против детей**[186]
    ИНТЕРПОЛ ведет работу по борьбе с теми преступлениями против детей, которые имеют международное измерение. Для помощи в поиске пропавших детей они выпускают «желтые уведомления», а их эксперты по борьбе с торговлей людьми сотрудничают со странами-членами для спасения детей, ставших жертвами торговли людьми и принудительного труда. Это подразделение также блокирует доступ к материалам по сексуальным надругательствам над детьми.

185. О нас, Internet Watch Foundation.
186. Кто мы такие, ИНТЕРПОЛ.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >



< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

5 Корпоративная ответственность

Предпринимательский сектор, включая некоммерческие организации, прямо и косвенно влияет на права детей при предоставлении услуг и продуктов, связанных с цифровой средой. Предприятия должны уважать права детей и предотвращать и устранять нарушения их прав в цифровой среде. Государства-участники должны обеспечить выполнение предприятиями этих обязанностей.

Государства-участники должны обеспечить, в том числе путем разработки, мониторинга, принятия и оценки законодательства, нормативных актов и политики, соблюдение предприятиями своих обязательств по предотвращению использования их сетей или онлайн-услуг для нарушения или ущемления прав детей, включая их права на конфиденциальность и защиту, и предоставить детям, родителям и опекунам быстрые и эффективные средства правовой защиты. Они также должны побуждать компании информировать общественность и предоставлять доступные и своевременные консультации для обеспечения безопасного и благоприятного для детей использования цифровых технологий.

Страны-участницы обязаны защищать детей от посягательств на их права со стороны коммерческих предприятий, включая право на защиту от всех форм насилия в цифровой среде. Такие предприятия часто не вовлечены в противоправную деятельность напрямую, однако могут являться причиной или способствовать нарушению прав детей на свободу от насилия, в том числе посредством разработки и оказания цифровых услуг. Странам-участницам следует контролировать и обеспечивать соблюдение законов и правил, предотвращающих нарушения прав на защиту от насилия, а также направленных на расследование, вынесение судебных решений и возмещение ущерба в связи с правонарушениями в цифровой среде.

Страны-участницы должны требовать от бизнес-сектора проведения юридической экспертизы в отношении прав ребенка, включая оценку воздействия, и предавать результаты гласности, уделяя особое внимание дифференцированному, а иногда и серьезному влиянию цифровой среды на детей. Им следует принять надлежащие меры для предупреждения, контроля и расследования нарушений прав ребенка со стороны коммерческих предприятий, а также наказания за них.

В дополнение к разработке законов и политик страны-участницы должны требовать от всех организаций, связанных с защитой прав ребенка в цифровой среде, применять нормативно-правовые рамки, отраслевые кодексы и условия предоставления услуг, соответствующие самым высоким стандартам этики, конфиденциальности и безопасности в отношении проектирования, разработки, использования, распространения и рекламы их продуктов и услуг. к числу таких организаций относятся те, которые ориентированы на детей, чьими конечными пользователями являются дети или которые иным образом связанные с детьми. От таких предприятий необходимо требовать поддержания высоких стандартов в отношении прозрачности и подотчетности, а также побуждать их к внедрению инноваций для наилучшего обеспечения интересов ребенка. Они также должны предоставлять соответствующие возрасту разъяснения в отношении условий использования их услуг детям, их родителям и опекунам.

Источник: Замечание общего порядка № 25 (2021 г.), пункты 35-39[187]

187. Замечание общего порядка № 25 (2021 год) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

5 Корпоративная ответственность

Цель

Содействовать разработке проектов, учитывающих интересы детей, минимальных стандартов, отраслевых соглашений, внедрению передовой практики, уважению культурных традиций и выделению ресурсов на обеспечение безопасности детей в Интернете путем нормативно-правового регулирования и создания программ в области корпоративной ответственности.

Текст типовой политики

Для обеспечения целостного подхода к безопасности детей в Интернете необходимо предпринять следующие шаги.

5a. Внедрить принципы встроенной безопасности, прав и этики
Следует создать стандарты и своды правил, требующие от разработчиков продуктов, производителей и поставщиков услуг защищать права ребенка и содействовать обеспечению безопасности детей в Интернете. Условия использования должны отвечать наилучшим интересам ребенка. в частности, стандарты и своды правил должны препятствовать предоставлению детям вредного или неподходящего для них контента или контактов; защищать конфиденциальность детей в Интернете на уровне системы или устройства; а также решать проблемы безопасности, возникающие в связи с Интернетом вещей (игрушками с выходом в Интернет и сервисами потоковой передачи). Они должны обязывать частные компании проводить оценку воздействия на права детей для учета рисков и смягчения последствий, направленную на предложение услуг, соответствующих возрасту.

5b. Ввести минимальные стандарты[188]
Отрасль несет ответственность за защиту детей в цифровой среде. Речь идет о создании безопасного и доступного для детей онлайн-пространства, а не только о предотвращении доступа к вредному контенту. На этапе создания онлайн-сервисов предприятия обязаны демонстрировать, какие процедуры и особые меры приняты для обеспечения безопасности детей и соблюдения их прав, используя систему оценки рисков 4C[189].[190] Свод правил должен быть разработан ведущим министерством или другим ведомством под надзором Руководящего комитета. Стандарты должны носить обязательный характер.

5c. Использовать возрастную классификацию
Использование единой возрастной классификации для коммерческого контента, средств массовой информации, игр и другой деятельности в Интернете обеспечивает прозрачный и эффективный подход к управлению информационными продуктами и сервисами, воздействующими на детей. Она может распространяться на связанные с детьми товары и услуги, а также контент, предназначенный для разных возрастных категорий. Для запрещенного контента или деятельности, не подходящей для ребенка, необходимо вводить ограничения по возрасту или создавать пространство только для взрослых. в частности, речь идет о контентной фильтрации, направленной на блокировку нежелательных материалов.[191]

5d. Внедрить системы модерации и отчетности
Поставщикам услуг необходимы механизмы для выявления подозрительного или неподходящего контента, а также прозрачные и надежные системы мониторинга для всех онлайн-сервисов, включая механизмы удаления. Для сообщения о нарушениях и получения доступа к специализированной поддержке и консультациям должна работать горячая линия. Механизмы отчетности должны быть легкодоступными для детей. в качестве дополнительного инструмента следует рассмотреть системы сообщения о нарушениях. ▶

188. См., например, Добровольные принципы противодействия сексуальной эксплуатации детей и жестокому обращению с ними в Интернете, GOV.UK, 2020 г.
189. См. раздел «Снижение рисков и вреда».
190. Оценка воздействия на права ребенка, Детский фонд Организации Объединенных Наций, 2013 г.
191. Откуда они знают, что речь идет о детях?, Фонд 5Rights, 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

5 Корпоративная ответственность

5e. Обеспечить защиту детей от коммерческого давления
Меры по защите детей от коммерческого давления должны включать поощрение проектов, учитывающих возрастные ограничения; предотвращение таргетированной рекламы и передачи информации третьим сторонам, а также повышение осведомленности об условиях, в которых растут дети. Продукты и услуги, которые учитывают права и повышают безопасность детей в Интернете, могут быть сертифицированы, а в отношении разработчиков, нарушающих эти принципы, могут быть приняты соответствующие меры.

5f. Обеспечить внедрение стандартов, учитывающих интересы детей, для минимизации рисков, связанных с безопасностью ребенка в Интернете
Например, речь идет о возможных контактах взрослых незнакомцев с детьми, таргетированной рекламе азартных игр или рекомендациях вредного контента. Принципы безопасности детей в Интернете должны быть внедрены на этапе проектирования, чтобы предотвратить дальнейшие потенциальные проблемы.

План мероприятий для достижения цели

A **Внедрить принципы встроенной безопасности, прав и этики**

Следует создать стандарты и своды правил, требующие от разработчиков продуктов, производителей и поставщиков услуг защищать права ребенка и содействовать обеспечению безопасности детей в Интернете. Условия использования должны отвечать наилучшим интересам ребенка. в частности, стандарты и своды правил должны препятствовать предоставлению детям вредного или неподходящего для них контента или контактов; защищать конфиденциальность детей в Интернете на уровне системы или устройства; а также решать проблемы безопасности, возникающие в связи с Интернетом вещей (игрушками с выходом в Интернет и сервисами потоковой передачи). Они должны обязывать частные компании проводить оценку воздействия на права детей для учета рисков и смягчения последствий, направленную на предложение услуг, соответствующих возрасту.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Определить нормативную или правовую возможность разработки кодекса поведения на принципах встроенной безопасности.
2. Определить регулирующий орган или ведомство, обладающие ресурсами и компетентностью для обеспечения соблюдения норм и контроля за их исполнением.
3. Разработать концепцию, ориентированную на встроенную безопасность и права: в качестве основы можно использовать, в частности, принцип встроенной безопасности[192].
4. Убедиться, что все заинтересованные стороны осведомлены о процессах (как технологических, так и управленческих), необходимых для создания концепции.
5. Проводить регулярный анализ возникающих вредных факторов и эффективности концепций, чтобы они учитывали инновации и коммерческую деятельность.

192. Встроенная безопасность, Комиссар по электронной безопасности, 2018 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

5 Корпоративная ответственность

B **Ввести минимальные стандарты**[193]

Отрасль несет ответственность за защиту детей в цифровой среде. Речь идет о создании безопасного и доступного для детей онлайн-пространства, а не только о предотвращении доступа к вредному контенту. На этапе создания онлайн-сервисов предприятия обязаны демонстрировать, какие процедуры и особые меры приняты для обеспечения безопасности детей и соблюдения их прав, используя систему оценки рисков 4C[194].[195]Свод правил должен быть разработан ведущим министерством или другим ведомством под надзором Руководящего комитета. Стандарты должны носить обязательный характер.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Ввести минимальные стандарты в областях, охватываемых вышеупомянутой концепцией. Определить подходящие модели[196], разработанные в других странах или регионах.
2. Проконтролировать соответствие минимальным стандартам в следующих областях: возрастные ограничения, модерация, условия использования или правила сообщества, процессы автоматического принятия решений и реклама. См. Средство поддержки 1 (стр. 109).

193. См., например, Добровольные принципы противодействия сексуальной эксплуатации детей и жестокому обращению с ними в Интернете, GOV.UK, 2020 г.
194. См. раздел «Риски и вред».
195. Оценка воздействия на права детей, Детский фонд Организации Объединенных Наций, 2013 г.
196. См., например, Добровольные принципы противодействия сексуальной эксплуатации детей и жестокому обращению с ними в Интернете, GOV.UK, 2020 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

5 Корпоративная ответственность

C **Использовать возрастную классификацию**

Использование единой возрастной классификации для коммерческого контента, средств массовой информации, игр и другой деятельности в Интернете обеспечивает прозрачный и эффективный подход к управлению информационными продуктами и сервисами, воздействующими на детей. Она может распространяться на связанные с детьми товары и услуги, а также контент, предназначенный для разных возрастных категорий. Для запрещенного контента или деятельности, не подходящей для ребенка, необходимо вводить ограничения по возрасту или создавать пространство только для взрослых. в частности, речь идет о контентной фильтрации, направленной на блокировку нежелательных материалов.[197]

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Найти подходящую услугу возрастной классификации информационной продукции. Во многих странах уже действует возрастная классификация для коммерческих фильмов[198] и/или игрушек. Те же критерии можно использовать для материалов и деятельности в Интернете.
2. Распространить требование к возрастной классификации контента и деятельности на цифровые технологии, включая приложения.
3. Обеспечить надзор за спорами и невыполнением обязательств со стороны соответствующего органа.

D **Внедрить системы модерации и отчетности.**

Поставщикам услуг необходимы механизмы для выявления подозрительного или неподходящего контента, а также прозрачные и надежные системы мониторинга для всех онлайн-сервисов, включая механизмы удаления. Для сообщения о нарушениях и получения доступа к специализированной поддержке и консультациям должна работать горячая линия. Механизмы отчетности должны быть легкодоступными для детей. в качестве дополнительного инструмента следует рассмотреть системы сообщения о нарушениях.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Установить минимальные стандарты, упомянутые в пункте A.
2. Определить ведомство, ответственное за общедоступную горячую линию.
3. Проконсультироваться с экспертами по вопросу обеспечения доступа детей к таким механизмам.

197. Откуда они знают, что речь идет о детях?, Фонд 5Rights, 2021.
198. См., например, Британский совет по классификации фильмов.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

5 Корпоративная ответственность

E **Обеспечить защиту детей от коммерческого давления**

Меры по защите детей от коммерческого давления должны включать поощрение проектов, учитывающих возрастные ограничения; предотвращение таргетированной рекламы и передачи информации третьим сторонам, а также повышение осведомленности об условиях, в которых растут дети. Продукты и услуги, которые учитывают права и повышают безопасность детей в Интернете, могут быть сертифицированы, а в отношении поставщиков, нарушающих эти принципы, могут быть приняты соответствующие меры.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Определить существующие законы и нормативные акты, касающиеся коммерческого взаимодействия с детьми: законодательство о защите ребенка, а также прав потребителей содержит ограничения в этой сфере, особенно в таких секторах, как здравоохранение или образование.
2. Упорядочить правила, чтобы они прямо распространялись на цифровые продукты и услуги.

F **Обеспечить внедрение стандартов, учитывающих интересы детей, для минимизации рисков, связанных с безопасностью ребенка в Интернете**

Например, речь идет о возможных контактах взрослых незнакомцев с детьми, таргетированной рекламе азартных игр или рекомендациях вредного контента. Принципы безопасности детей в Интернете должны быть внедрены на этапе проектирования, чтобы предотвратить дальнейшие потенциальные проблемы.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

Рассмотреть возможность внедрения принципов встроенной безопасности[199] в конкретных областях, которые могут затрагивать детей непреднамеренно, включая азартные игры для взрослых, финансовые услуги, порнографию или другие сайты, неподходящие для детей.

199. Откуда они знают, что речь идет о детях?, Фонд 5Rights, 2021.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

5 Корпоративная ответственность

Как это согласуется с основополагающими документами

Общие функции государств в сфере нормативного регулирования и политики

При выполнении своей обязанности по обеспечению защиты государствам следует:

(a) обеспечивать исполнение законов, направленных на то, чтобы требовать от коммерческих предприятий соблюдения прав человека, и периодически оценивать адекватность таких законов и устранять любые пробелы;

(b) обеспечивать, чтобы другие законы и политики, регулирующие создание и текущую деятельность коммерческих предприятий, такие как нормы корпоративного права, не сдерживали, а, наоборот, способствовали соблюдению прав человека такими предприятиями;

(c) предоставлять коммерческим предприятиям эффективные руководящие указания относительно способов соблюдения прав человека в рамках их деятельности;

(d) поощрять и, при необходимости, требовать от коммерческих предприятий представления информации о том, каким образом они устраняют оказанное ими негативное воздействие на права человека.

Источник: Руководящие принципы предпринимательской деятельности в аспекте прав человека, Организация Объединенных Наций, 2011 г., раздел 3[200]

При регулировании рекламных и маркетинговых кампаний, предназначенных для детей или доступных им, странам-участницам следует ориентироваться прежде всего на наилучшее обеспечение интересов ребенка. Платная и скрытая реклама, а также другие формы коммерческого контента должны быть четко отделены от всех прочих материалов и не должны поддерживать гендерные или расовые стереотипы.

Замечание общего порядка № 25 (2021 г.), пункт 41[201]

Странам-участницам следует законодательно запретить составление профилей детей любого возраста или таргетирование в коммерческих целях с использованием цифровых записей об их фактических или предполагаемых характеристиках, включая групповые данные, таргетированные на основе коллективных или похожих профилей. Деятельность по продвижению продуктов, приложений и услуг, связанная с нейромаркетингом, эмоциональной аналитикой, иммерсивной рекламой или рекламой в виртуальной и дополненной реальности, также не должна напрямую или косвенно затрагивать детей.

Источник: Замечание общего порядка № 25 (2021 г.), пункт 42[202]

Средства поддержки

1. Этапы разработки цифровых продуктов и услуг с учетом прав детей

Фонд 5Rights и Ассоциация стандартов Института инженеров электротехники и электроники (IEEE-SA) разработали стандарт, предусматривающий практические шаги, которым компании могут следовать для разработки цифровых продуктов и услуг с учетом возраста пользователей. в нем описан ряд процессов, которые на этапе разработки позволят поставить потребности молодых людей на первое место.

200. Руководящие принципы предпринимательской деятельности в аспекте прав человека, Управление Верховного комиссара Организации Объединенных Наций по правам человека, 2011 г.
201. Замечание общего порядка № 25 (2021 год) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.
202. Замечание общего порядка № 25 (2021 год) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

5 Корпоративная ответственность

Прочие справочные ресурсы

1. Пример того, что молодые люди думают о корпоративной ответственности

Молодые люди, с которыми общались эксперты 5Rights, ждут от компаний следующего:

- Единые правила сообщества, распространяющиеся на всех пользователей платформы
- Четкие сроки предоставления отчетности
- Возможность сообщить жертве о том, какие меры приняты в отношении нарушителя
- Более четкая маркировка контента
- Простые способы удаления контента
- Запрет на распространение насилия
- Всплывающие уведомления, напоминающее о правильном поведении и использовании конфиденциальных настроек
- Четкое описание процессов подачи жалоб
- Простые для понимания политики

2. Руководящие указания по вопросам подотчетности частного сектора, Принципы предпринимательской деятельности в аспекте прав детей, Организация Объединенных Наций[203]

Частный сектор также несет ответственность за безопасность детей в Интернете, и эти обязательства должны быть четко отражены в соответствующих областях политики. Некоторые аспекты, такие как кибербуллинг, CSEA, а также финансовое мошенничество, связаны с конкретным нормативно-правовым регулированием, обеспечивающим безопасности детей в Интернете, но существуют и всеобъемлющие концепции в области корпоративной ответственности.

Принципы предпринимательской деятельности в аспекте прав детей требуют от всех предприятий:

- ☐ Выполнять свою обязанность в отношении соблюдения прав детей и взять на себя обязательство по поддержке прав человека.
- ☐ Содействовать борьбе с детским трудом во всех секторах предпринимательской деятельности и коммерческих отношениях.
- ☐ Обеспечить достойную работу молодым работникам, родителям и опекунам.
- ☐ Обеспечивать защиту и безопасность детей в рамках всех видов предпринимательской деятельности и на предприятиях.
- ☐ Обеспечить безопасность продуктов и услуг, а также стремиться поддерживать права детей с помощью таких продуктов и услуг.
- ☐ Использовать маркетинговые инструменты и рекламу, которые уважают и поддерживают права детей.
- ☐ Уважать и поддерживать права детей в отношении окружающей среды, а также приобретения и использования земли.
- ☐ Уважать и поддерживать права детей в рамках мероприятий по обеспечению безопасности.
- ☐ Содействовать защите прав детей, пострадавших от чрезвычайных ситуаций.
- ☐ Активизировать усилия сообществ и правительства в области защиты и осуществления прав детей.

203. Принципы предпринимательской деятельности в аспекте прав детей: обязанности и действия, Международная комиссия юристов и Детский фонд Организации Объединенных Наций, 2015 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

3. **Замечание общего порядка № 16 (2013 г.) об обязательствах государств, касающихся воздействия предпринимательской деятельности на права детей**[204]
   Руководство Комитета Организации Объединенных Наций по правам ребенка, касающееся обязательств государств в отношении воздействия предпринимательской деятельности и коммерческих операций на права детей.

4. **Разъяснения в отношении принципов предпринимательской деятельности в аспекте прав детей**[205]
   Более доступная для чтения версия Замечания общего порядка № 16 (2013 г.) Комитета по правам ребенка об обязательствах государств в отношении воздействия предпринимательской деятельности на права детей.

5. **Руководящие принципы предпринимательской деятельности в аспекте прав детей**[206]
   Документ, разработанный ЮНИСЕФ, Глобальным договором Организации Объединенных Наций и Save the Children, представляет собой всеобъемлющий свод принципов и мер, которые компании должны принимать на рабочих местах, торговых платформах и в сообществе в целях обеспечения соблюдения и поддержки прав детей.

6. **Принципы предпринимательской деятельности в аспекте прав детей: обязанности и действия**[207]
   Практическое руководство для государств по осуществлению Замечания общего порядка № 16 (2013 г.) Комитета Организации Объединенных Наций по правам ребенка.

7. **IEEE 2089-2021 Стандарт для нормативного регулирования цифровых услуг с учетом возраста**[208]
   Фонд 5Rights и Ассоциация стандартов Института инженеров электротехники и электроники (IEEE-SA) разработали стандарт, предусматривающий практические шаги, которым компании могут следовать для разработки цифровых продуктов и услуг с учетом возраста пользователей.

8. **Руководство ЮНИСЕФ по использованию инструмента оценки безопасности детей в Интернете. Расширение прав и возможностей технологических компаний в целях создания безопасной цифровой среды для детей**[209]
   Руководство ЮНИСЕФ по использованию инструмента оценки безопасности детей в Интернете помогает предприятиям в подготовке и выполнении оценки воздействия их деятельности на детей. в нем описываются цель, правовая база и функции инструмента оценки безопасности детей в Интернете, а также предлагаются подробные инструкции и рекомендации по его использованию.

9. **Безопасность детей в Интернете. Практическое руководство для платформ социальных сетей и поставщиков интерактивных услуг**[210]
   Руководство правительства Великобритании, созданное на основе концепции безопасности в рамках европейской отраслевой инициативы ICT Coalition for Children Online и предназначенное для поставщиков социальных сетей. Его цель — сделать платформы более безопасными для пользователей.

204. Замечание общего порядка № 16 (2013 г.) об обязательствах государств, касающихся воздействия предпринимательской деятельности на права детей, Конвенция Организации Объединенных Наций о правах ребенка, 2013 г.
205. Разъяснения принципов предпринимательской деятельности в аспекте прав детей, Детский фонд Организации Объединенных Наций и Save the Children, 2015 г.
206. Принципы предпринимательской деятельности в аспекте прав детей, Детский фонд Организации Объединенных Наций, Глобальный договор Организации Объединенных Наций и Save the 8 Children, 2013 г.
207. Принципы предпринимательской деятельности в аспекте прав детей: обязанности и действия, Международная комиссия юристов и Детский фонд Организации Объединенных Наций, 2015 г.
208. Стандарт для нормативного регулирования цифровых услуг с учетом возраста IEEE 2089-21, IEEE SA, 2021 г.
209. Руководство по использованию инструмента оценки безопасности детей в Интернете, Детский фонд Организации Объединенных Наций, 2016 г.
210. Безопасность детей в Интернете. Практическое руководство для платформ социальных сетей и поставщиков интерактивных услуг, Департамент Великобритании по цифровым технологиям, культуре, СМИ и спорту, 2016 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

10. **Доклад «Откуда они знают, что речь идет о детях?», Фонд 5Rights**[211]
    Доклад Фонда 5Rights, посвященный обсуждению вопросов проверки, оценки и учета возраста пользователей.

11. **Итальянский свод правил в отношении кибербуллинга**[212]
    Официальный свод правил итальянского правительства по кибербуллингу (на итальянском языке).

12. **Финансовая коалиция против детской порнографии**[213]
    В докладе описываются методы, применяемые некоторыми членами Финансовой коалиции против детской порнографии, процессы их проверки и использования для выявления материалов, связанных с сексуальным насилием над детьми, и предотвращения открытия или поддержания коммерческих аккаунтов, связанных с распространением и продажей таких материалов.

13. **Коммерческая сексуальная эксплуатация детей в Интернете, 2015 г.**[214]
    Доклад Европейской финансовой коалиции против коммерческой сексуальной эксплуатации детей в Интернете представляет собой обновленный вариант Стратегической оценки коммерческой сексуальной эксплуатации детей в Интернете, опубликованной в октябре 2013 года в нормативном документе Европейской финансовой коалиции. Помимо фактов и цифр 2013 года, в нем также приведены другие важные аспекты в этой области.

14. **Всеобщая декларация «Безопасность детей в Интернете»**[215]
    Декларация Комиссии по широкополосной связи, цель которой — донести важность общей миссии по защите детей в Интернете до всех заинтересованных сторон.

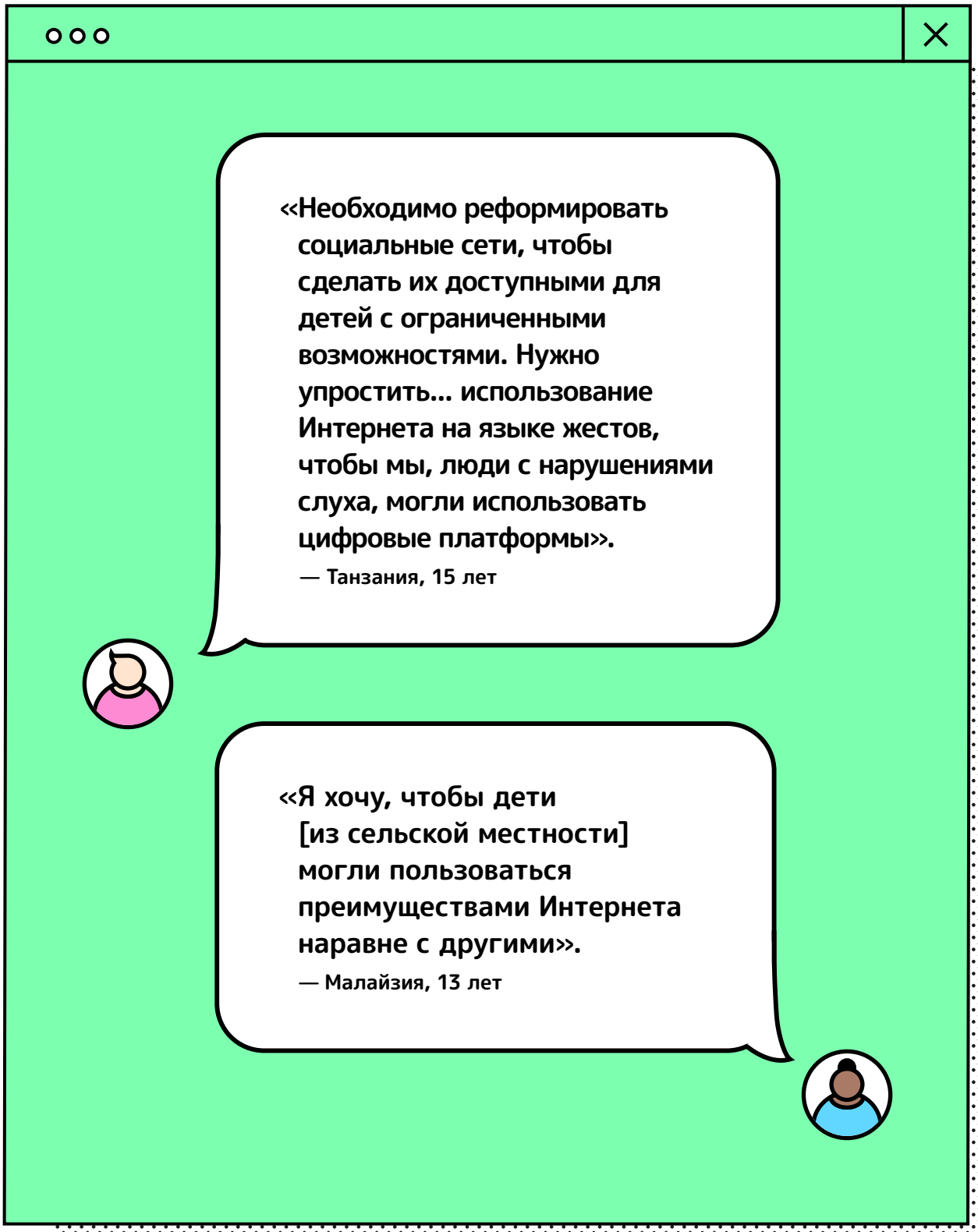
15. **Трилогия о перспективных практиках ЮНИСЕФ в Албании**[216]
    Тематическое исследование, проведенное в Албании. Четыре из пяти крупнейших компаний, занимающихся вопросами Интернета и связи, приняли участие в процессе разработки отраслевых руководящих принципов, опубликованных Национальным управлением электронной сертификации и кибербезопасности.

16. **Руководство ОЭСР для поставщиков цифровых услуг**[217]
    Эти руководящие принципы призваны дополнить рекомендации Совета по правам детей в цифровой среде [СНОСКА 2] и помочь поставщикам цифровых услуг определить наилучшие способы защиты и соблюдения прав, безопасности и интересов ребенка в рамках их деятельности, которая может прямо или косвенно затрагивать детей.

211. Откуда они знают, что речь идет о детях?, Фонд 5Rights, 2021 г.
212. Положения о защите несовершеннолетних в целях предупреждения кибербуллинга и борьбе с ним, Gazzetta Ufficiale, 2017 г.
213. Проверка новых интернет-продавцов и передовые практики мониторинга, способствующие сокращению распространения коммерческой детской порнографии, Международный центр по делам пропавших без вести и эксплуатируемых детей, 2016 г.
214. Коммерческая сексуальная эксплуатация детей в Интернете, Европол, 2015 г.
215. Всеобщая декларация «Безопасность детей в Интернете», Комиссия по широкополосной связи, 2019 г.
216. Разработка албанской программы защиты детей в Интернете, Детский фонд Организации Объединенных Наций, 2020 г.
217. Руководство ОЭСР для поставщиков цифровых услуг, ОЭСР, 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >



«Необходимо реформировать социальные сети, чтобы сделать их доступными для детей с ограниченными возможностями. Нужно упростить... использование Интернета на языке жестов, чтобы мы, люди с нарушениями слуха, могли использовать цифровые платформы».

— Танзания, 15 лет

«Я хочу, чтобы дети [из сельской местности] могли пользоваться преимуществами Интернета наравне с другими».

— Малайзия, 13 лет

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

6 Обучение

> **Специалисты, работающие с детьми и для них, а также представители бизнес-сектора, включая технологическую отрасль, должны проходить подготовку, включающую изучение того, как цифровая среда влияет на права ребенка в различных контекстах, как дети осуществляют в ней свои права и как они получают доступ к технологиям и используют их. Они также должны пройти обучение по вопросам применения международных стандартов в области прав человека в цифровой среде. Странам-участницам следует обеспечить обучение по вопросам, касающимся цифровой среды, для специалистов на всех уровнях системы образования как до начала, так и в процессе работы в целях расширения их знаний и практических навыков в этой области.**
>
> Источник: Замечание общего порядка № 25 (2021 г.), пункт 33[218]

Цель

Обеспечить четкое понимание принципов безопасности ребенка в Интернете и наилучших интересов детей для всех, кто связан с услугами, касающимися детей, включая правительство, правоохранительные органы, судебную систему, здравоохранение, политиков и должностных лиц, а также тех, кто занимается разработкой технологий.

Текст типовой политики

Для обеспечения целостного подхода к безопасности детей в Интернете необходимо предпринять следующие шаги.

6a. Обеспечить обучение, развитие навыков и подготовку для всех, кто связан с безопасностью детей в Интернете
Все участники правоохранительной системы и специалисты, работающие с детьми в таких сферах, как образование и здравоохранение: от сотрудников экстренных служб до судей, — должны быть осведомлены о безопасности детей в Интернете. Необходимо провести для них всестороннее обучение, в том числе по вопросам о том, как безопасность детей в Интернете связана с их конкретными обязанностями, как определить противоправное поведение и предоставить помощь жертвам.

6b. Провести специализированное обучение по вопросу психосоциальной поддержки и выявлению всего спектра проблем, связанных с безопасностью детей в Интернете
Чтобы выполнять свои обязанности эффективным образом, специалисты-практики должны проходить обучение по вопросам безопасности детей в Интернете, политик, обеспечивающих защиту детей, а также консультирования детей и семей. Вопросы безопасности ребенка в Интернете должны быть включены в существующие программы в области защиты детей. Специалисты, работающие с детьми в образовательных, медицинских, общественных и других учреждениях, должны научиться распознавать признаки и симптомы проблем, связанных с безопасностью в Интернете.

6c. Создать обучающие программы в системе высшего специального образования
Занятия по вопросам безопасности детей в Интернете должны стать обязательной частью учебных программ государственных и частных университетов или других учебных заведений, готовящих учителей, медицинских работников, психологов и других специалистов. Необходимо проводить регулярную оценку эффективности этого обучения с учетом новой информации и проблем, связанных с безопасностью детей в Интернете. Учебные планы должны охватывать все аспекты безопасности детей в Интернете, как указано в настоящей политике. ▶

218. Замечание общего порядка № 25 (2021 год) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

6 Обучение

6d. Поощрять профессиональное развитие

Чтобы идти в ногу с новыми технологиями и устранять препятствия и проблемы по мере их появления, программы непрерывного обучения по вопросам безопасности детей в Интернете для специалистов в соответствующих областях должны регулярно пересматриваться и обновляться.

План мероприятий для достижения цели

A **Обеспечить обучение, развитие навыков и подготовку для всех, кто связан с безопасностью детей в Интернете**

Все участники правоохранительной системы и специалисты, работающие с детьми в таких сферах, как образование и здравоохранение: от сотрудников экстренных служб до судей, — должны быть осведомлены о безопасности детей в Интернете. Необходимо провести для них всестороннее обучение, в том числе по вопросам о том, как безопасность детей в Интернете связана с их конкретными обязанностями, как определить противоправное поведение и предоставить помощь жертвам.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Определить круг специалистов и других лиц, которым может потребоваться обучение по вопросам безопасности детей в Интернете. в этом может помочь средство поддержки 1 (см. стр. 119).
2. Проанализировать существующие учебные программы и определить, на каком этапе и уровне требуется внедрить детальное обучение по вопросам безопасности детей в Интернете (см. раздел «Ресурсы» ниже).
3. Поручить разработку плана обучения или обновить существующую учебную программу по вопросам безопасности детей в Интернете с учетом конкретной специальности. Для обеспечения высококачественного обучения такие материалы могут носить междисциплинарный характер.
4. Обеспечить успешное прохождение обучения в любой области.
5. Обеспечить регулярное обновление учебных материалов и охватить все аспекты жизни ребенка в Интернете: контент, контакты, поведение и коммерческие риски.
6. Рассмотреть вопрос о том, как учесть в обучении мнение детей и молодежи.[219]

219. См., например, Модель участия детей Ланди, Европейская комиссия, 2007 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

6 Обучение

B **Провести специализированное обучение по вопросу психосоциальной поддержки и выявлению всего спектра проблем, связанных с безопасностью детей в Интернете**

Чтобы выполнять свои обязанности эффективным образом, специалисты-практики должны проходить обучение по вопросам безопасности детей в Интернете, политик, обеспечивающих защиту детей, а также консультирования детей и семей. Вопросы безопасности ребенка в Интернете должны быть включены в существующие программы в области защиты детей. Специалисты, работающие с детьми в образовательных, медицинских, общественных и других учреждениях, должны научиться распознавать признаки и симптомы проблем, связанных с безопасностью в Интернете, выявлять неправомерное поведение и оказывать поддержку жертвам.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Определить круг лиц, которым требуется обучение в области психосоциальной поддержки и противодействия сексуальной эксплуатации детей и жестокому обращению с ними (CSEA).
2. Утвердить полностью проверенную программу обучения как на международном, так и на региональном уровне (см. пункты 1–4 раздела «Прочие справочные ресурсы»).
3. Выделить достаточные финансовые ресурсы и время для обучения по вопросам противодействия сексуальной эксплуатации детей и жестокому обращению с ними (CSEA).
4. Определить, когда и как будет проводиться, оцениваться и улучшаться обучение.
5. Рассмотреть вопрос о том, как учесть в обучении мнение детей и молодежи.[220]
6. Создать систему KPI в рамках обучения специалистов для регулярной оценки его эффективности и отчетности.

220. См., например, Модель участия детей Ланди, Европейская комиссия, 2007 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

6 Обучение

C **Создать обучающие программы в системе высшего специального образования**

Занятия по вопросам безопасности детей в Интернете должны стать обязательной частью учебных программ государственных и частных университетов или других учебных заведений, готовящих учителей, медицинских работников, психологов и других специалистов. Необходимо проводить регулярную оценку эффективности этого обучения с учетом новой информации и проблем, связанных с безопасностью детей в Интернете. Учебные планы должны охватывать все аспекты безопасности детей в Интернете, как указано в настоящей политике.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, могут быть полезны примеры, приведенные в пункте 1 раздела «Прочие справочные ресурсы» (см. ниже).

D **Поощрять профессиональное развитие**

Чтобы идти в ногу с новыми технологиями и устранять препятствия и проблемы по мере их появления, программы непрерывного обучения по вопросам безопасности детей в Интернете для специалистов в соответствующих областях должны регулярно пересматриваться и обновляться.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Обеспечить доступность обучения на протяжении всего цикла трудовой деятельности и обновлять его с учетом изменений как в цифровом мире, так и в обязанностях специалиста.
2. Определить возможности для дальнейшего обучения.
3. Разработать план углубленного или дополнительного обучения (см. пункты 1–4 раздела «Прочие справочные ресурсы»).
4. Рассмотреть вопрос о том, как учесть в обучении мнение молодых людей.[221]

221. См., например, Модель участия детей Ланди, Европейская комиссия, 2007 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

6 Обучение

Как это согласуется с основополагающими документами

Странам-участницам следует рассмотреть вопрос о том, каким образом использование цифровых технологий может способствовать или препятствовать расследованию преступлений против детей и судебному преследованию за них, и принять все имеющиеся превентивные, правоприменительные и коррективные меры в этом отношении, в том числе в сотрудничестве с международными партнерами. Они должны обеспечить специализированное обучение сотрудников правоохранительных органов, прокуроров и судей по вопросам нарушений прав ребенка, непосредственно связанных с цифровой средой, в том числе в рамках международного сотрудничества.

Источник: Замечание общего порядка № 25 (2021 г.), пункт 47[222]

222. Замечание общего порядка № 25 (2021 год) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

6 Обучение

Средства поддержки

1. Контрольный список профессий, которым может быть полезно специализированное обучение, и темы для рассмотрения

Его цель — помочь вам определить, актуальна ли существующая программа обучения для специалистов в вашей области, и выявить возможные пробелы. Данное средство поддержки должно использоваться в рамках достижения цели A («Обеспечить обучение, развитие навыков и подготовку для всех, кто связан с безопасностью детей в Интернете»).

Профессия	Обучение по всем вопросам безопасности детей в Интернете и использованию системы оценки рисков 4C	Обучение по вопросам политики в области обеспечения защиты	Понимание проблем безопасности детей в Интернете	Понимание поведения правонарушителей и их реабилитация	Психологическая помощь	Оказание поддержки жертвам
Судьи	[указать существующий план обучения или пробелы]					
Правоохранители						
Социальные работники						
Медицинские работники						
Учителя						
Специалисты, работающие в условиях сообщества						
Психологи						
Другие						

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

6 Обучение

Прочие справочные ресурсы

Существует множество примеров учебных онлайн-модулей, доступных для различных групп специалистов. Ознакомительная, непрерывная подготовка и обучение в системе высшего специального образования должны предоставляться широкому кругу специалистов, включая учителей/педагогов, сотрудников правоохранительных органов, работников судебной системы, социальных и медицинских работников, специалистов по работе с молодежью, парламентариев, должностных лиц, технических специалистов (включая программистов, дизайнеров пользовательского интерфейса и администраторов), а также сотрудникам регулирующих органов в соответствующих областях.

1. **Ресурсы для учителей, социальных работников и специалистов по работе с молодежью**
   См. обучение по безопасности в Интернете Национального общества предупреждения жестокого обращения с детьми (NSPCC). Все, кто работает с детьми и молодежью, должны знать, что делать, если ребенок обращается к ним с вопросом, связанным с контентом в Интернете. Это обучение призвано помочь профессионалам расширить свои знания в области безопасности детей в Интернете.[223]

2. **Ресурсы для медицинских работников**
   Обучение eIntegrity по вопросам защиты детей в Интернете для медицинских работников («Защита детей и молодежи») предоставляет знания и навыки, необходимые медицинским и социальным работникам для обеспечения благополучия детей. Программа была разработана консорциумом профессиональных организаций под руководством Королевского колледжа педиатрии и здоровья детей.[224]

   Данный курс по безопасности в Интернете включен в британскую программу обучения в этой области — межвузовский документ «Защита детей и молодежи: обязанности и области компетенции медицинского персонала» (2019 г.).[225] Однако охваченные в нем вопросы актуальны для специалистов в области здравоохранения и социальной защиты во всем мире.[226]

3. **Ресурсы для правоохранителей[227]**
   Международный центр по делам пропавших без вести и эксплуатируемых детей (ICMEC) предоставляет широкий спектр различных обучающих программ и курсов, таких как:

   - Основы преступлений против детей, совершаемых при техническом содействии
   - Расширенный анализ случаев эксплуатации в Интернете
   - Передовые технологии
   - Основы реагирования на проблему пропавших без вести детей.

223. Ознакомительное обучение по вопросам обеспечения безопасности и защиты детей, Национальное общество предупреждения жестокого обращения с детьми.
224. Обучение по вопросам защиты детей в Интернете для медицинских работников, eIntegrity.
225. Защита детей и молодежи: обязанности и области компетенции, Королевский колледж педиатрии и здоровья детей, 2019 г.
226. Обучение по вопросам защиты детей в Интернете для медицинских работников, eIntegrity.
227. Создание глобального потенциала для защиты детей, Международный центр по делам пропавших без вести и эксплуатируемых детей, 2015 г., и ресурсы ICMEC, Международный центр по делам пропавших без вести и эксплуатируемых детей.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

4. **Гендерное насилие в Намибии: исследовательская оценка и обзор служб реагирования на гендерное насилие в Виндхуке, 2016 г.**[228]
   В Намибии Группа по защите от гендерного насилия (GBVPU) и программы подготовки детей-свидетелей предоставляют обучение для следователей, прокуроров, магистратов и социальных работников (сотрудников по вопросам защиты детей) для обеспечения более эффективной всесторонней поддержки жертв. GBVPU доступна для людей с ограниченными возможностями, включает удобное для детей помещение для проведения видеоинтервью и следует стандартным операционным процедурам в отношении гендерного насилия (ГН) над детьми и VAC.

5. **Ресурсы для сотрудников судебной системы**[229]
   Подготовка судей и прокуроров по вопросам, касающимся противодействия сексуальной эксплуатации детей и жестокому обращению с ними (CSEA), обеспечивается в рамках проекта EndOCSEA Совета Европы.

6. **Общие ресурсы**
   Комиссия Квинсленда по делам семьи и детей подготовила онлайн-модуль по вопросам защиты детей.[230]

228. Гендерное насилие в Намибии: исследовательская оценка и обзор служб реагирования на гендерное насилие в Виндхуке, Victims 2 Survivors и ЮНЭЙДС, 2016 г.
229. Противодействие сексуальной эксплуатации детей и жестокому обращению с ними в Интернете, Совет Европы, 2021 г.
230. Онлайн-модуль «Защита детей», Комиссия Квинсленда по делам семьи и детей, 2022 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

7 Образовательные программы

> **Странам-участницам следует поддерживать создание адаптированного к возрасту и не нарушающего права цифрового контента для детей в соответствии с этапами их развития и их обеспечивать доступ к широкому спектру информации, включая сведения государственных органов, о культуре, спорте, искусстве, здравоохранении, гражданских и политических вопросах и правах ребенка.**
>
> **Странам-участницам следует поощрять производство и распространение такого контента в различных форматах и из множества национальных и международных источников, включая средства массовой информации, вещательные компании, музеи, библиотеки, а также образовательные, научные и культурные организации. Они должны, в частности, стремиться к распространению разнообразного, доступного и полезного контента для детей-инвалидов и детей, принадлежащих к этническим, языковым, национальным и другим группам меньшинств. Возможность доступа к нужной информации на языках, которые понимают дети, может оказать значительное позитивное воздействие на обеспечение равенства.**
>
> Источник: Замечание общего порядка № 25 (2021 г.), пункты 51 и 52[231]

Цель

Отстаивать безопасное и позитивное использование цифровых технологий в качестве источника развлечений, информации и обучения для детей.

Текст типовой политики

Для обеспечения целостного подхода к безопасности детей в Интернете необходимо предпринять следующие шаги.

7a. Назначить ведущего специалиста по охране прав детей

Каждая школа должна назначить ведущего специалиста по охране прав детей.[232] Такие специалисты должны пройти обучение в области процедур защиты детей и безопасности детей в Интернете. Ведущие специалисты будут отвечать за принятие, введение в действие и применение в школах правил безопасности детей в Интернете (включая процедуры безопасности и анонимного сообщения о нарушениях). Также они должны выступать в качестве контактных лиц по вопросам, касающимся защиты детей и их безопасности в Интернете, и передавать сообщения о причиненном вреде соответствующим органам. Кроме того, ведущим специалистам следует содействовать осуществлению планов мероприятий, направленных на защиту детей от любого вреда.

7b. Содействовать развитию доступного цифрового образования

Необходимо продвигать контент, в том числе программы «равные равным», направленный на развитие цифровых навыков и расширение возможностей детей в создании сообществ, в которых действует атмосфера взаимного уважения и поддерживается их безопасность в Интернете. Комплексная программа цифрового образования должна охватывать темы, связанные с данными, использованием социальных сетей и защитой. в частности речь идет о вопросах, касающихся сексуальной жизни и согласия. Необходимо также обеспечить обучение родителей/опекунов, чтобы они могли успешно следить за безопасностью своих детей в Интернете. ▶

231. Замечание общего порядка № 25 (2021 г.) о правах детей в отношении цифровой среды, Комитет Организации Объединенных Наций по правам ребенка, 2021 г.
232. В качестве специалиста могут выступать участники школьного комитета по безопасности, педагог или представитель местного комитета по защите детей, в котором представлены школы.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

7 Образовательные программы

7c. Продвигать образовательный контент
По мере распространения цифровых технологий ученики и учителя должны обучаться необходимым навыкам взаимодействия с цифровыми системами, чтобы пользоваться всеми преимуществами учебных программ как на местном, так и на международных языках.

7d. Повышать осведомленность по вопросам данных
В школьный учебный план должны быть введена программа обучения по вопросам данных. в рамках этой программы дети получат знания о том, как может быть использована их информация, и базовое понимание экономики данных. Ее цели — продвигать позитивное, автономное и творческое использование цифровых технологий детьми; четко определить риски, выгоды и социальные результаты использования таких технологий; а также обеспечить широкое распространение, понимание и применение защитных и профилактических мер в этой сфере. Обучение по вопросам данных должно четко определять круг заинтересованных сторон, отвечающих за безопасность в Интернете.

7e. Поощрять критическое мышление
Обучение критическому мышлению и повышение осведомленности о рисках, связанных с дезинформацией в Интернете, должны быть включены в образовательные программы в области компьютерной грамотности. Такое обучение должно включать вопросы прав человека, в частности, прав ребенка, и то, как они применяются в Интернете и в реальной жизни.[233]

7f. Ввести в школах формальные процедуры обеспечения безопасности детей в Интернете
Подготовка по вопросам безопасности детей в Интернете должна составлять обязательную часть педагогического образования как на уровне начальной, так и средней школы, а также стать одним из основных направлений непрерывного обучения учителей без отрыва от основной работы. Все учителя должны пройти обязательное обучение в области безопасности детей в Интернете, ознакомиться со школьной политикой в этом отношении и проводить на эту тему занятия для учеников. Чтобы следить за соблюдением стандартов и школьной политики в отношении безопасности детей в Интернете, школы должны назначить ведущего специалиста в этой области.

233. См. статью 29 Конвенции о правах ребенка и соответствующие разделы Замечания общего порядка.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

7 Образовательные программы

План мероприятий для достижения цели

A Назначить ведущего специалиста по охране прав детей

Каждая школа должна назначить ведущего специалиста по охране прав детей.[234] Такие специалисты должны пройти обучение в области процедур защиты детей и безопасности детей в Интернете. Ведущие специалисты будут отвечать за принятие и применение политики в области защиты детей (включая процедуры безопасности и анонимного сообщения о нарушениях) в школах. Они должны выступать в качестве контактных лиц по вопросам, касающимся защиты детей и их безопасности в Интернете, и передавать сообщения о причиненном вреде соответствующим органам. Кроме того, ведущим специалистам следует содействовать осуществлению планов мероприятий, направленных на защиту детей от любого вреда.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Определить действующую в школе политику и правила в области защиты ребенка и убедиться, что они включают разделы, связанные с безопасностью детей в Интернете. Если их не существует, следует обратиться к передовым практикам. См. примеры 1–6 в разделе «Прочие ресурсы».
2. В любом случае подготовка к каждому учебному году должна включать в себя принятие обновленных мер по защите и обеспечению безопасности детей и ознакомление с ними всех учителей школы. См. пункт 2 раздела «Прочие ресурсы», в котором приведены онлайн-курсы, доступные для рядовых работников.

234. В качестве специалиста могут выступать участники школьного комитета по безопасности, педагог или представитель местного комитета по защите детей, в котором представлены школы.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

7 Образовательные программы

B **Содействовать развитию доступного цифрового образования**

Необходимо продвигать контент, в том числе программы «равные равным», направленный на развитие цифровых навыков и расширение возможностей детей в создании сообществ, в которых действует атмосфера взаимного уважения и поддерживается их безопасность в Интернете. Комплексная программа цифрового образования должна охватывать темы, связанные с данными и цифровой грамотностью, включая вопросы, касающиеся сексуальной жизни и согласия. Необходимо также обеспечить обучение родителей/опекунов, чтобы они могли успешно следить за безопасностью своих детей в Интернете.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Убедиться в том, что обучение компьютерной грамотности охватывает все аспекты взаимодействия с Интернетом, а не только вопросы безопасности. Это связано с тем, что многие дети, не уделяющие внимание цифровой защите, стремятся к более широкому пониманию возможностей и рисков в этой сфере. Ознакомиться с моделью DQ (см. пункт 3 раздела «Прочие ресурсы»), демонстрирующей области, которые необходимо охватить (см. «Ресурсы» ниже), и убедиться, что любые области с возможными рисками охватывают все аспекты системы 4C (см. раздел «Выявление рисков и смягчение вреда»).
2. Обеспечить, чтобы вопросы полового воспитания, сексуальности и согласия преподносились в контексте цифрового мира. Это позволит предоставить детям весь набор возможностей для решения соответствующих проблем, которые могут возникнуть в Интернете.
3. Определить программы компьютерной грамотности на нужном языке или, при необходимости, найти те, что доступны для перевода.[235]
4. Обеспечить соответствие программ компьютерной грамотности для родителей/опекунов и детей. Ресурсы для родителей должны быть полными и носить позитивный характер, чтобы не вызывать излишней паники в том, что касается цифрового мира, и не поощрять принятие радикальных мер в отношении детей.[236]
5. Проверить технологические компании, предлагающие бесплатные программы компьютерной грамотности как для детей, так и для взрослых. Часто такие программы очень эффективны, однако компании не в состоянии определить коммерческие риски и вред, связанные с самой технологией. Если на местном уровне принято решение об их использовании, важно убедиться, что они охватывают все аспекты риска, включая те, что вызваны самими программами.

235. См., например, программу «Компьютерная грамотность» Международного союза электросвязи.
236. См., например, «Компьютерная грамотность: ресурсы для родителей», Образовательный фонд Джорджа Лукаса, 2012 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

7 Образовательные программы

C **Продвигать образовательный контент**

По мере распространения цифровых технологий ученики и учителя должны обучаться необходимым навыкам взаимодействия с цифровыми системами, чтобы пользоваться всеми преимуществами учебных программ как на местном, так и на иностранных языках.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Определить качественный образовательный контент, связанный с учебной программой или внеклассной деятельностью школы.
2. Обеспечить, чтобы условия использования соответствовали стандартам конфиденциальности и безопасности учащихся.
3. Убедиться, что все учащиеся, независимо от пола, инвалидности и социально-экономического статуса, получают доступ к ресурсам: речь может идти о возможностях подключения, доступности (включая данные) и доступа к необходимым устройствам.
4. Провести проверку ресурсов от авторитетных учреждений (например, университетов, школ, НПО), предлагаемых на различные темы и из различных источников. в некоторых случаях может быть эффективнее потратиться на перевод или использовать существующие материалы вместо того, чтобы создавать их с нуля. в других случаях лучше вложить средства в разработку или использование материалов на местных языках, охватывающих аспекты местной культуры или истории.
5. Важно понять, что широко доступные онлайн-материалы включают аспекты, выходящие за пределы квалифицированного обучения, доступного на местном уровне. Однако бывают случаи, когда специально подготовленный педагог может предоставить более качественное онлайн-обучение.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

7 Образовательные программы

D **Повышать осведомленность по вопросам данных**

В школьный учебный план должны быть введена программа обучения по вопросам данных. в рамках этой программы дети получат знания о том, как может быть использована их информация, и базовое понимание экономики данных. Ее цели — продвигать позитивное, автономное и творческое использование цифровых технологий детьми; четко определить риски, выгоды и социальные результаты использования таких технологий; а также обеспечить широкое распространение, понимание и применение защитных и профилактических мер в этой сфере. Обучение по вопросам данных должно четко определять круг заинтересованных сторон, отвечающих за безопасность в Интернете.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно рассмотреть ресурсы и меры, упомянутые в пунктах A-C выше.

E **Поощрять критическое мышление**

Обучение критическому мышлению и повышение осведомленности о рисках, связанных с дезинформацией в Интернете, должны быть включены в образовательные программы в области компьютерной грамотности. Такое обучение должно включать вопросы прав человека, в частности, прав ребенка, и то, как они применяются в Интернете и в реальной жизни.[237]

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно рассмотреть ресурсы и меры, упомянутые в пунктах A-C выше.

237. См. статью 29 Конвенции о правах ребенка и соответствующие разделы Замечания общего порядка.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

7 Образовательные программы

F **Ввести в школах формальные процедуры обеспечения безопасности детей в Интернете**

Подготовка по вопросам безопасности детей в Интернете должна составлять обязательную часть педагогического образования как на уровне начальной, так и средней школы, а также стать одним из основных направлений непрерывного обучения учителей без отрыва от основной работы. Все учителя должны пройти обязательное обучение в области безопасности детей в Интернете, ознакомиться со школьной политикой в этом отношении и проводить на эту тему занятия для учеников. Чтобы следить за соблюдением стандартов и школьной политики в отношении безопасности детей в Интернете, школы должны назначить ведущего специалиста в этой области.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно рассмотреть ресурсы и меры, упомянутые в пунктах A-C выше.

Как это согласуется с основополагающими документами

Обучение детей компьютерной грамотности является частью стратегии, направленной на то, чтобы они могли пользоваться преимуществами технологий без каких-либо рисков. Оно позволяет детям развивать навыки критического мышления и помогает определять положительные и отрицательные аспекты своего поведения в цифровом пространстве. Несмотря на важность демонстрации вреда, с которым дети могут столкнуться в Интернете, она будет эффективной только при включении этого аспекта в более широкую программу компьютерной грамотности, которая должна соответствовать возрасту и концентрироваться на развитии знаний и навыков. в подготовку по вопросам безопасности в Интернете необходимо включить аспекты социального и эмоционального обучения: это поможет учащимся понимать свои эмоции и управлять ими, что важно для построения здоровых и уважительных отношений как в цифровой среде, так и за ее пределами.

Источник: Руководящие указания для директивных органов по защите ребенка в онлайновой среде, Международный союз электросвязи, 2020 г.[238]

Обеспечение всеохватного и справедливого качественного образования и поощрение возможности обучения на протяжении всей жизни для всех.

Источник: Цель в области устойчивого развития № 4[239]

238. Руководящие указания для директивных органов по защите ребенка в онлайновой среде, Международный союз электросвязи, 2020 г.
239. Цель 4: обеспечение всеохватного и справедливого качественного образования и поощрение возможности обучения на протяжении всей жизни для всех, Организация Объединенных Наций, 2017 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

7 Образовательные программы

Средства поддержки

1. Контрольный список для введения в школах формальных процедур обеспечения безопасности детей в Интернете

Его цель — выявление пробелов в действующих в школе процедурах обеспечения безопасности детей в Интернете. Контрольный список можно использовать для отслеживания прогресса в достижении цели F («Ввести в школах формальные процедуры обеспечения безопасности детей в Интернете»).

Вопрос	Ответ
Входят ли вопросы безопасности детей в Интернете в программу учебных курсов для учителей?	
Назначен ли ведущий специалист по вопросам безопасности детей в Интернете во всех начальных и средних учебных заведениях?	
Все ли начальные и средние школы имеют политику в области безопасности детей в Интернете?	
Все ли начальные школы проводят курсы по безопасности в Интернете для учащихся? a. Назначить ведущего специалиста по охране прав детей b. Содействовать развитию доступного цифрового образования c. Продвигать образовательный контент d. Повышать осведомленность по вопросам данных e. Поощрять критическое мышление f. Ввести в школах формальные процедуры обеспечения безопасности детей в Интернете	
Все ли средние школы проводят курсы по безопасности в Интернете для учащихся?	

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

Прочие справочные ресурсы

1. **DQ Child Digital Readiness Kit: 8-дневное домашнее электронное обучение для детей (в возрасте 8–12 лет) и родителей**[240]
   Восьмидневная программа электронного обучения, в рамках которой дети могут получить 8 навыков цифрового гражданства при минимальной поддержке со стороны родителей или учителей. По завершении каждого модуля родители получают по электронной почте оценочную карточку цифрового интеллекта, в которой подробно описан прогресс их ребенка и его подверженность киберугрозам. Также им предоставляется электронная копия «Справочника для родителей по цифровому интеллекту».

2. **Безопасность детей в Интернете, Южная Африка**[241]
   Сайт содержит интерактивные рекомендации в отношении безопасности детей в Интернете, предназначенные для педагогов и лиц, осуществляющих уход за детьми. На платформе лица, осуществляющие уход за детьми, и работники сферы образования могут обмениваться информацией о своих стратегиях или школьной политике в этой области.

3. **Национальная ассоциация школьных психологов: концепция безопасной и успешной школы**[242]
   Документ содержит рекомендации о том, как повысить физическую и психологическую безопасность детей и молодежи на основе стратегии создания безопасных и комфортных школ.

4. **Международная целевая группа по защите детей: международные стандарты и рекомендации в области защиты детей**[243]
   В этом докладе, подготовленном Комитетом по оценке школ, излагаются требования в отношении оценки школ по вопросам защиты детей для аккредитационных и инспекционных учреждений.

5. **Совет международных школ**[244]
   Сайт содержит полезные рекомендации и инструменты для лиц, осуществляющих уход за детьми, и преподавателей по вопросам безопасности детей и молодежи. На нем приведены примеры семинаров по вопросам защиты детей, психического здоровья и благополучия, стандартов безопасного найма и т. д.

6. **Обучение по вопросам безопасности в Интернете от Национального общества предупреждения жестокого обращения с детьми (на английском языке)** [245]
   Этот онлайн-курс предлагает обучение по различным аспектом безопасности ребенка в Интернете для лиц, осуществляющих уход за детьми. Он включает в себя такие важные проблемные области, как радикализация, экстремизм, буллинг и сексуальные преступления в цифровом пространстве. ▶

240. Глобальное движение за цифровое гражданство для детей в возрасте от 8 до 12 лет, Институт DQ.
241. Безопасность детей в Интернете, образовательный портал Thutong.
242. Концепция безопасной и успешной школы, Национальная ассоциация школьных психологов, 2013 г.
243. Обновленные стандарты в области защиты детей, принятые учреждениями по оценке школ, Международный центр по делам пропавших без вести и эксплуатируемых детей, 2021 г.
244. Ресурсы Совета международных школ.
245. Ознакомительное обучение по вопросам обеспечения безопасности и защиты детей, Национальное общество предупреждения жестокого обращения с детьми.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

7. Примеры образовательных ресурсов на тему безопасности детей в Интернете

A. Пример учебной программы: Young and eSafe от Австралийского управления Комиссара по электронной безопасности[246]
На сайте представлены короткие видеоролики и другой образовательный контент, который помогает молодым людям получить информацию о правильном поведении в Интернете.

B. Бесплатные уроки по цифровому гражданству для детей любого возраста от Common Sense Education[247]
На сайте представлены бесплатные уроки, которые помогут детям и подросткам получить навыки цифрового гражданства. Среди прочего, они охватывают такие темы, как кибербуллинг и конфиденциальность в Интернете.

C. Рабочая тетрадь по безопасности в Интернете от Международного союза электросвязи[248]
Рабочая тетрадь содержит основные положения Конвенции о правах ребенка и некоторые упражнения по безопасному взаимодействию с людьми в Интернете.

D. Руководство для учителей от Международного союза электросвязи[249]
Руководство содержит инструкции и ресурсы для классных занятий по безопасности в Интернете с детьми от 9 до 12 лет. Цель занятий — вдохновить учащихся и учителей на обсуждение проблем, связанных с безопасностью в Интернете, и поиск способов их решения.

E. Digiworld от МСЭ: пример того, как руководящие принципы Международного союза электросвязи по защите детей в Интернете могут быть реализованы на практике[2 50]
В документе рассматривается, как на практике использовать принципы МСЭ для развития навыков безопасности детей в Интернете.

F. Международный набор обучающих средств Childnet[251]
The Step Up, Speak Up! Набор обучающих средств — это практический, интерактивный и основанный на сценариях ресурс, в котором рассматривается проблема сексуальных домогательств в Интернете среди детей от 13 до 17 лет. Он состоит из 4 планов уроков с сопроводительными фильмами, аудиофайлами, семинарами и презентацией собрания.

G. Руководство «Обучение онлайн-безопасности в школе», Великобритания[252]
Руководство для школ, которое помогает им обучать учеников безопасности в Интернете в рамках новых и существующих школьных предметов.

H. Буклет и видео Kiko and the Manymes от EndOCSEA, Совет Европы[253]
Книга рассказов и видео, выпущенная Советом Европы, представляет собой руководство по безопасному использованию Интернета как для лиц, осуществляющих уход, так и для маленьких детей.

246. Young and eSafe, Управление Комиссара по электронной безопасности.
247. Всё, что нужно знать для обучения цифровому гражданству, Common Sense Education.
248. Рабочая тетрадь по безопасности в Интернете Work with Sango, Международный союз электросвязи.
249. Рабочая тетрадь по безопасности в Интернете: руководство для учителей, Международный союз электросвязи.
250. Digiworld: пример того, как руководящие принципы МСЭ по защите детей в Интернете могут быть реализованы на практике, Международный союз электросвязи, 2020 г.
251. Набор обучающих средств, Childnet.
252. Преподавание онлайн-безопасности в школе, Департамент образования, 2019.
253. Мероприятия EndOCSEA@Europe: Kiko's exciting adventures continue in the digital age, Совет Европы, 2020 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

8. **Кампания WebFighter, Шри-Ланка**[254]
   Сайт содержит полезные рекомендации и инструменты для лиц, осуществляющих уход за детьми, и преподавателей по вопросам безопасности детей и молодежи. На нем приведены примеры семинаров по вопросам защиты детей, психического здоровья и благополучия, стандартов безопасного найма и т. д.

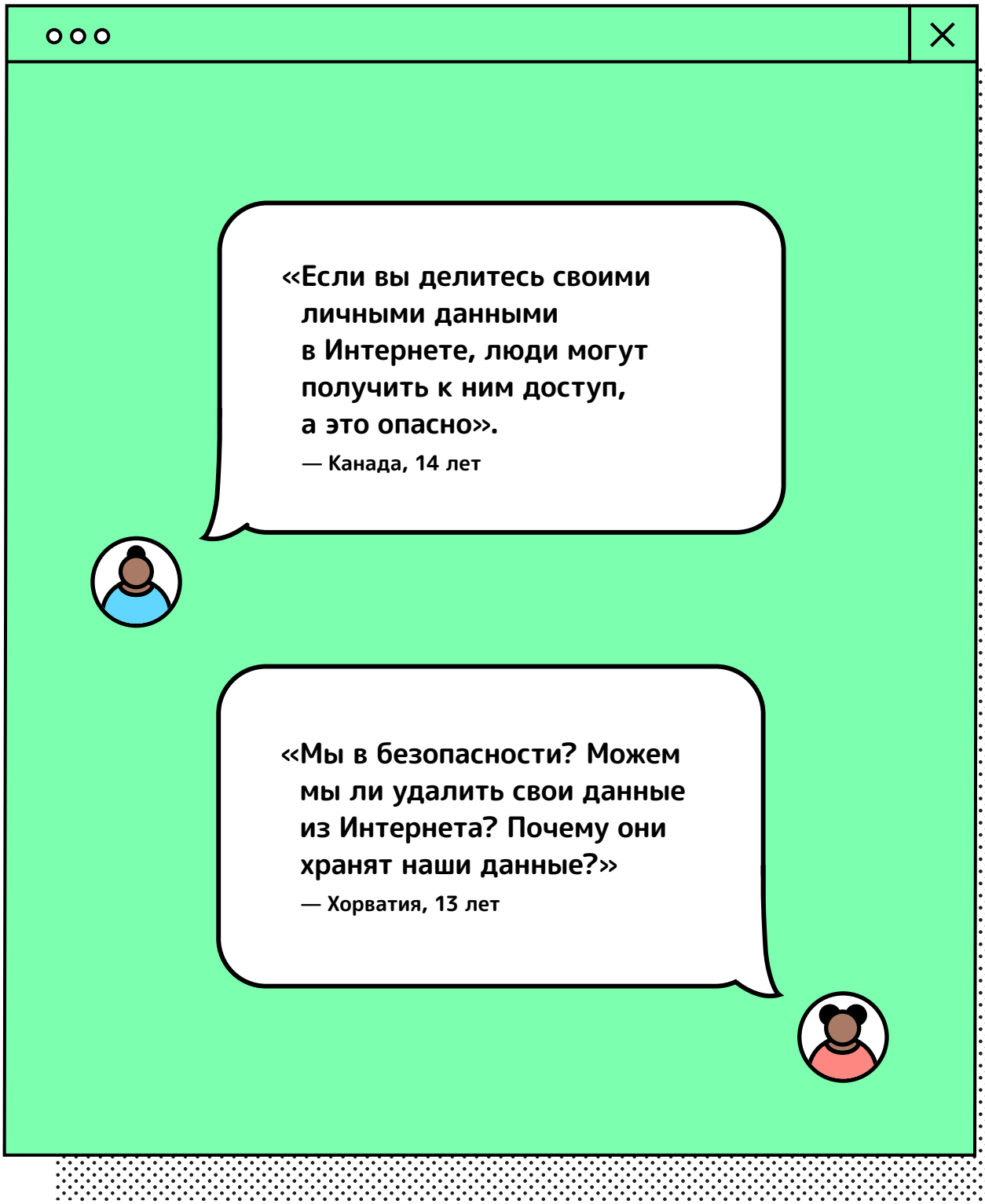
9. **Программа Swipe Safe**[255]
   Программа помогает молодым людям безопасно пользоваться Интернетом, информируя их о таких потенциальных рисках, как кибермошенничество, буллинг и сексуальные домогательства, и предлагая им стратегии защиты. Эта учебная программа была адаптирована неправительственными организациями для применения во Вьетнаме, Лаосе и Мьянме. Swipe Safe мобилизует родителей, молодежь, школы и частный сектор, позволяя им играть более активную роль в обеспечении безопасности детей в Интернете. Программа предусматривает обучение владельцев/управляющих интернет-кафе по вопросам выявления и устранения рисков и возможных неблагоприятных событий, которые могут произойти с детьми в цифровой среде и за ее пределами. Она также оказывает поддержку школам в разработке учитывающих интересы детей стратегий и руководящих указаний по вопросам безопасности в Интернете.

10. **Digital Literacy Package (DLP)**[256]
    Подготовленный ЮНИСЕФ Ганский пакет компьютерной грамотности был разработан для того, чтобы научить детей навыкам компьютерной грамотности и обеспечить их безопасность и устойчивость к угрозам в Интернете. Он также содержит компоненты, ориентированные на родителей/опекунов. Эти материалы помогают им поддерживать безопасность детей в Интернете, особенно в условиях COVID-19, когда дистанционное обучение стало нормой.

254. Институт Гёте.
255. Swipe Safe от ChildFund, ChildFund Alliance, 2019 г.
256. Digital Literacy Package (DLP), ЮНИСЕФ, 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >



< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

8 Связи с общественностью и формирование коллективной сознательности

> **Странам-участницам следует распространять информацию и проводить кампании по повышению осведомленности о правах ребенка в цифровой среде, уделяя особое внимание тем, чьи действия прямо или косвенно затрагивают детей. Они должны продвигать образовательные программы для детей, родителей и опекунов, широкой общественности и законодателей в целях расширения их знаний о правах детей в отношении возможностей и рисков, связанных с цифровыми продуктами и услугами. Такие программы должны включать информацию о том, каким образом дети могут извлекать пользу из цифровых продуктов и услуг и развивать свою компьютерную грамотность и навыки, как защитить частную жизнь ребенка и предотвратить виктимизацию, а также как распознать ребенка, который является жертвой преступления, совершенного в Интернете или за его пределами, и надлежащим образом отреагировать на эту ситуацию. Программы должны основываться на результатах исследований и консультаций с детьми, родителями и опекунами.**
>
> Источник: Замечание общего порядка № 25 (2021 г.), пункт 32[257]

Цель

Повысить осведомленность обо всех проблемах безопасности детей в Интернете во всех секторах общества, чтобы предотвратить возможный вред и способствовать позитивному использованию Интернета. Эта информация должна широко распространяться с помощью специальных программ, предназначенных для различных аудиторий.

Текст типовой политики

Для обеспечения целостного подхода к безопасности детей в Интернете необходимо предпринять следующие шаги.

8a. Разработать программу повышения осведомленности

Стратегии повышения осведомленности помогут людям понять проблему безопасности детей в Интернете и ориентироваться в ней, продолжая при этом пользоваться преимуществами цифрового пространства. в подготавливаемых материалах должны быть четко изложены принципы безопасности детей в Интернете и действия, которые могут быть предприняты для понимания риска, снижения вреда, сообщения о правонарушениях и требования возмещения. Данная информация будет представлена в простой форме на официальных сайтах. Целевые сообщения и материалы должны разрабатываться на основе консультаций с детьми, молодежью и родителями/опекунами. в них следует учитывать особые потребности родителей/опекунов и детей, уделяя особое внимание самым маленьким и наиболее уязвимым детям, включая детей с особыми образовательными потребностями или без родительского попечения. Метод обучения «равный равному» является ценной стратегией для детей всех возрастов, позволяющей им ознакомиться со своими правами и обязанностями в Интернете. Эта программа публично распространяемых сообщений поможет детям и взрослым понять проблемы и сделать разумный выбор в отношении их взаимодействия в Интернете, но не заменяет официальное образование, профессиональную подготовку, принцип встроенной безопасности или программу корпоративной ответственности. Такая информация должна охватывать весь спектр вопросов безопасности детей в Интернете, как указано в настоящей политике.

257. Замечание общего порядка № 25 (2021 г.) о правах детей в отношении цифровой среды,Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

8 Связи с общественностью и формирование коллективной сознательности

Пять межсекторальных вопросов

1. Как выявлять риски и смягчать их последствия
2. Как обеспечить доступ к информационным технологиям, доступность информации и взаимодействие всех заинтересованных сторон
3. Как построить цепочку ответственности и сотрудничества
4. Как добиться того, чтобы проект учитывал интересы детей
5. Как обеспечить эффективность системы

Десять областей применения политики

1. Возможности вовлеченных организаций
2. Нормативно-правовое регулирование
3. Персональные данные, идентичность и самостоятельность
4. Системы реагирования и поддержки
5. Корпоративная ответственность
6. Обучение
7. Образовательные программы
8. Связи с общественностью и формирование коллективной сознательности
9. Научно-исследовательская работа
10. Международное сотрудничество

8b. Предоставить доступную информацию и учебные материалы

Обучение по вопросам безопасности в Интернете должно начинаться в раннем детстве и развиваться в соответствии с меняющимися потребностями ребенка по мере его взросления: необходимо подготовить специальные руководства для детей всех возрастов, их семей и лиц, осуществляющих уход. Информационные материалы должны продвигать позитивное использование цифровых технологий, учитывать вопросы сексуальности и согласия, а также потребности всех детей, независимо от гендера, возраста, дохода или происхождения. Информация, предоставляемая третьими сторонами, должна отражать принципы защиты детей и помогать ребенку любого возраста узнавать о рисках и своих правах в Интернете. в материалах необходимо подчеркивать мысль о том, что дети и пользователи не несут ответственности за плохие вещи, которые с ними происходят. Группы по интересам, молодежные клубы, семьи, религиозные учреждения и цифровые платформы будут играть важную роль в эффективном повышении осведомленности о безопасности детей в Интернете и неофициальном обучении на уровне сообщества.

8c. Повысить осведомленность о безопасности детей в Интернете в средствах массовой информации

Следует предоставить средствам массовой информации материалы по вопросам безопасности детей в Интернете для их освещения в удобной для детей форме. СМИ и развлекательные компании должны быть осведомлены о безопасности детей в Интернете. Кроме того, где это уместно, их необходимо поощрять к оказанию сбалансированной, ответственной и содержательной поддержки кампаниям по повышению осведомленности общественности. Необходимо поощрять публикации по всему спектру вопросов безопасности детей в Интернете, а не только наиболее драматичные заголовки, связанные с этим.

8d. Привлекать родителей/опекунов и детей к обсуждению вопросов безопасности детей в Интернете

Родители/опекуны и другие члены семьи должны иметь возможность понимать и принимать меры по обеспечению безопасности детей в Интернете в собственном доме. Для эффективного выявления проблем, поиска решений и путей повышения осведомленности о безопасности детей в Интернете необходимо провести консультации с семьями и детьми.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

8 Связи с общественностью и формирование коллективной сознательности

План мероприятий для достижения цели

A **Разработать программу повышения осведомленности**

Стратегии повышения осведомленности помогут людям понять проблему безопасности детей в Интернете и ориентироваться в ней, продолжая при этом пользоваться преимуществами цифрового пространства. в подготавливаемых материалах должны быть четко изложены принципы безопасности детей в Интернете и действия, которые могут быть предприняты для понимания риска, снижения вреда, сообщения о правонарушениях и требования возмещения. Данная информация будет представлена в простой форме на официальных сайтах.

Целевые сообщения и материалы должны разрабатываться на основе консультаций с детьми, молодежью и родителями/опекунами. в них следует учитывать особые потребности родителей/опекунов и детей, уделяя особое внимание самым маленьким и наиболее уязвимым детям, включая детей с особыми образовательными потребностями или без родительского попечения. Метод обучения «равный равному» является ценной стратегией для детей всех возрастов, позволяющей им ознакомиться со своими правами и обязанностями в Интернете. Эта программа публично распространяемых сообщений поможет детям и взрослым понять проблемы и сделать разумный выбор в отношении их взаимодействия в Интернете, но не заменяет официальное образование, профессиональную подготовку, принцип встроенной безопасности или программу корпоративной ответственности. Такая информация должна охватывать весь спектр вопросов безопасности детей в Интернете, как указано в настоящей политике.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Определить ключевые аудитории и понять, как они воспринимают данную тему и какие сомнения испытывают.
2. Определить основные идеи, которые нужно донести до каждой аудитории. См. Средство поддержки 1.
3. Подумать, как сообщение может способствовать безопасному использованию цифровых технологий, а не просто шокировать или вызвать беспокойство у читателя.
4. Обеспечить, чтобы сообщения не носили дискриминационный характер, например, не создавали впечатление о том, что девочкам не стоит пользоваться Интернетом или что онлайн-общение с людьми другого происхождения представляет опасность.
5. Сотрудничать с детьми и родителями/опекунами для улучшения и/или тестирования своих сообщений.
6. Учесть, что разные аудитории требуют разного набора сообщений.[258]

258. См., например, Политику Руанды в отношении защиты детей в Интернете, Фонд 5Rights, 2019 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

8 Связи с общественностью и формирование коллективной сознательности

B **Предоставить доступную информацию и учебные материалы**

Обучение по вопросам безопасности в Интернете должно начинаться в раннем детстве и развиваться в соответствии с меняющимися потребностями ребенка по мере его взросления: необходимо подготовить специальные руководства для детей всех возрастов, их семей и лиц, осуществляющих уход. Информационные материалы должны продвигать позитивное использование цифровых технологий и учитывать потребности всех детей, независимо от гендера, возраста, дохода или происхождения. Информация, предоставляемая третьими сторонами, должна отражать принципы защиты детей и помогать ребенку любого возраста узнавать о своих правах в Интернете. в материалах необходимо подчеркивать мысль о том, что дети и пользователи не несут ответственности за плохие вещи, которые с ними происходят. Группы по интересам, молодежные клубы, семьи, религиозные учреждения и цифровые платформы будут играть важную роль в эффективном повышении осведомленности о безопасности детей в Интернете и неофициальном обучении на уровне сообщества.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Определить ключевые аудитории.
2. Определить основные идеи, которые нужно донести до каждой аудитории.
3. Подумать, как сообщение может способствовать безопасному использованию цифровых технологий, а не просто шокировать или вызвать беспокойство у читателя.
4. Обеспечить, чтобы сообщения не носили дискриминационный характер, например, не создавали впечатление о том, что девочкам не стоит пользоваться Интернетом или что онлайн-общение с людьми другого происхождения представляет опасность.
5. Ознакомиться с примерами разных аудиторий и сообщений.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

8 Связи с общественностью и формирование коллективной сознательности

C **Повысить осведомленность о безопасности детей в Интернете в средствах массовой информации**

Следует предоставить средствам массовой информации материалы по вопросам безопасности детей в Интернете для их освещения в удобной для детей форме. СМИ и развлекательные компании должны быть осведомлены о безопасности детей в Интернете. Кроме того, где это уместно, их необходимо поощрять к оказанию сбалансированной, ответственной и содержательной поддержки кампаниям по повышению осведомленности общественности. Необходимо поощрять публикации по всему спектру вопросов безопасности детей в Интернете, а не только наиболее драматичные заголовки, связанные с этим.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Поручить ведущему министерству и руководящему органу разработку ключевых сообщений и KPI на основе Набора программных средств для обеспечения безопасности детей в Интернете.
2. Повышать уровень осведомленности и понимания проблемы, а также призывать средства массовой информации внимательно относиться к используемым формулировкам. Там, где позволяют ресурсы, проводить обучение для работников средств массовой информации.
3. Обеспечить публикацию сообщений как со стороны основных, так и со стороны специализированных СМИ в целях вызвать интерес общественности и обеспечить информированность о выполнении плана мероприятий, включая успехи, а также любые задержки или трудности.
4. Убедиться, что ключевые заинтересованные стороны и политические лидеры готовы продвигать план мероприятий в области безопасности детей в Интернете и принимать участие в его выполнении.[259]

259. Политика Руанды в отношении защиты детей в Интернете, 5Rights Foundation, 2019 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

8 Связи с общественностью и формирование коллективной сознательности

D **Привлекать родителей/опекунов и детей к обсуждению вопросов безопасности детей в Интернете**

Родители/опекуны и другие члены семьи должны иметь возможность понимать и принимать меры по обеспечению безопасности детей в Интернете в собственном доме. Для эффективного выявления проблем и путей повышения осведомленности о безопасности детей в Интернете необходимо проводить консультации с семьями и детьми.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Определить правительственные департаменты, НПО и специалистов, которые работают с детьми, семьями и опекунами или прямо контактируют с ними.
2. Предоставить им возможность принять участие в выполнении плана мероприятий и обеспечить понимание сферы его действия.
3. Учитывать мнения детей, родителей/опекунов при составлении информационных материалов и руководств.
4. Составить ключевые сообщения для семей и опекунов, отражающие их сомнения, но в то же время расширяющие их знания в области цифровой среды; учесть мнения детей, которые они высказывают непосредственно своим родителям/опекунам.[260]

260. Наши права в цифровом мире, Фонд 5Rights, 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

8 Связи с общественностью и формирование коллективной сознательности

Как это согласуется с основополагающими документами

Диапазон целей кибератак постоянно увеличивается. Новые интернет-пользователи, как правило, плохо осведомлены о цифровой гигиене. Уже более половины атак направлены на элементы Интернета вещей, которые включают большой спектр устройств от смарт-телевизоров до детских мониторов и термостатов. Высокоскоростные сети 5G будут и дальше интегрировать Интернет с физической инфраструктурой, что может привести к появлению новых уязвимостей.

Источник: Эпоха цифровой взаимозависимости, Группа высокого уровня Генерального секретаря ООН по цифровому сотрудничеству, 2019 г.[261]

Странам-участницам следует обеспечить, чтобы компьютерная грамотность преподавалась в школах в рамках базовых учебных программ от дошкольных учреждений и на протяжении всех школьных лет и чтобы такие методики преподавания оценивались на основе полученных результатов. Учебные программы должны включать знания и навыки в области безопасного использования широкого спектра цифровых инструментов и ресурсов, в том числе связанные с контентом, его созданием, сотрудничеством, участием, социализацией и гражданской активностью. Учебные программы также должны быть направлены на развитие критического мышления, навыков поиска надежных источников информации, выявления ложных сведений и других форм необъективного или ложного контента, в том числе по вопросам сексуального и репродуктивного здоровья, прав человека, включая права ребенка в цифровой среде, и имеющихся форм поддержки и средств правовой защиты. Они должны содействовать повышению осведомленности детей о возможных неблагоприятных последствиях рисков, связанных с контентом, контактами, поведением и договорами, включая киберагрессию, торговлю людьми, сексуальную эксплуатацию, домогательства и другие формы насилия; информированию о стратегиях снижения вреда, защиты собственных личных данных и данных других лиц; а также развитию у детей социальных и эмоциональных навыков и устойчивости к рискам.

Источник: Замечание общего порядка № 25 (2021 г.), пункт 104[262]

261. Эпоха цифровой взаимозависимости, Группа высокого уровня Генерального секретаря ООН по цифровому сотрудничеству, 2019 г.
262. Замечание общего порядка № 25 (2021 год) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

8 Связи с общественностью и формирование коллективной сознательности

Средства поддержки

1. Контрольный список для обеспечения комплексности программы по повышению осведомленности

Цель a («Разработать программу повышения осведомленности») требует разработки общей программы повышения осведомленности, которая может быть ориентирована на некоторые конкретные аудитории. Данный инструмент поможет вам проконтролировать соблюдение этих требований.

Группа/аудитория	Основное послание для их охвата
Дети младше 12 лет	
Дети 12–18 лет	
Уязвимые дети: — на попечении; — с особыми потребностями; — с языковыми барьерами; — участники системы уголовного правосудия; — не охваченные системой общего образования.	
Семьи с особыми потребностями	
Семьи, проживающие в сельских и отдаленных районах	

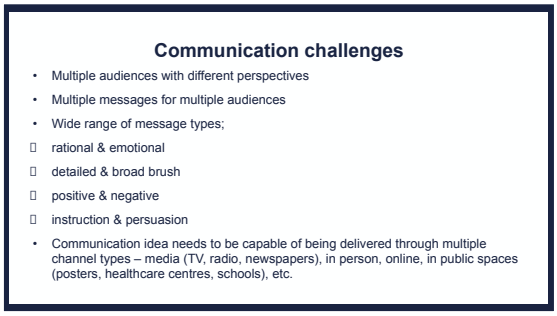
< ПРЕДЫДУЩИЙ РАЗДЕЛ

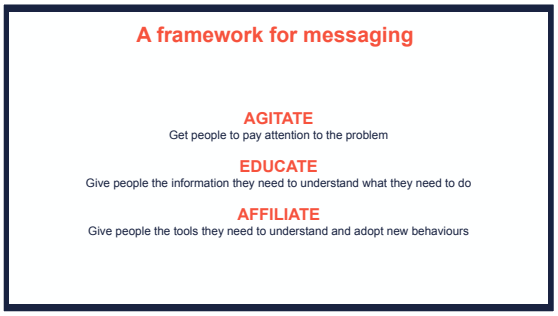
СЛЕДУЮЩИЙ РАЗДЕЛ >

8 Связи с общественностью и формирование коллективной сознательности

Прочие справочные ресурсы

1. **Защита детей в Интернете, Руанда. Информационные материалы по защите детей в Интернете**[263]
   По поручению правительства Руанды Фонд 5Rights подготовил ряд информационных материалов в рамках осуществления политики обеспечения безопасности детей в Интернете.





263. Защита детей в Интернете, Руанда, Фонд 5Rights, 2019 г.

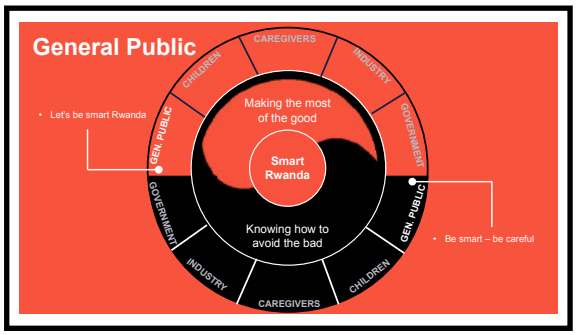
< ПРЕДЫДУЩИЙ РАЗДЕЛ

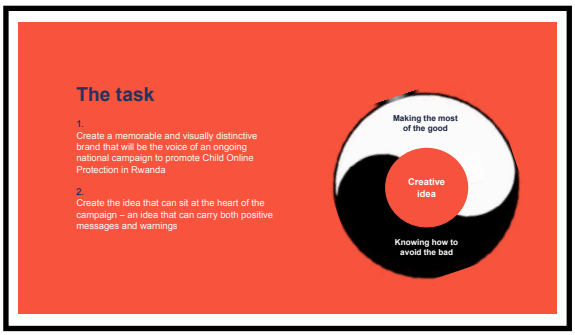
СЛЕДУЮЩИЙ РАЗДЕЛ >

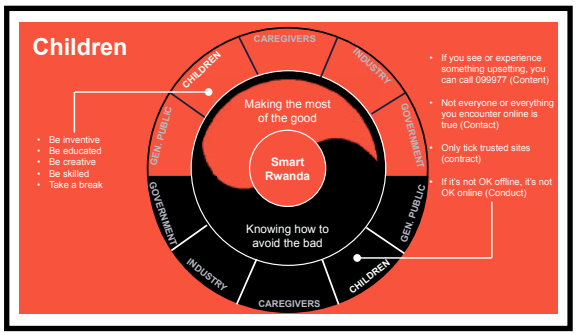
8 Связи с общественностью и формирование коллективной сознательности

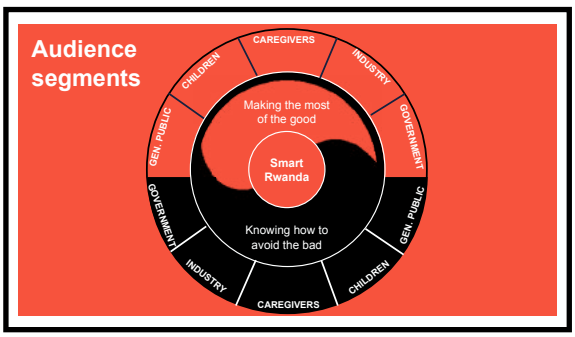
The right message will contain both silver lining and cloud

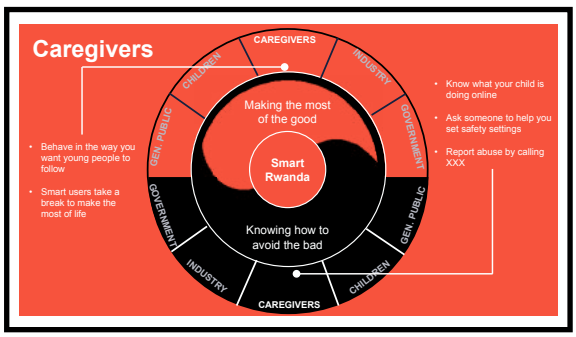
Messaging by segment (illustrative)







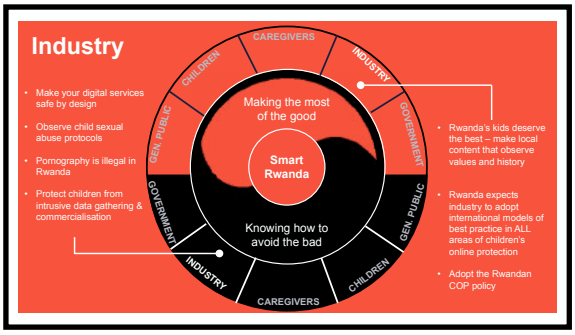


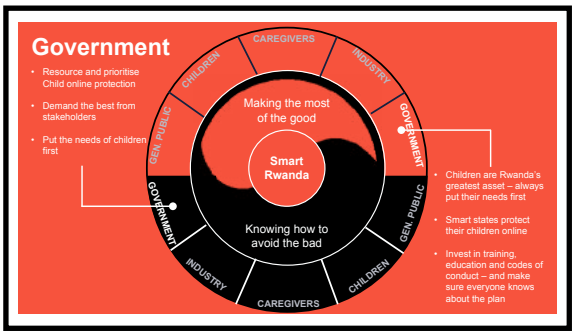


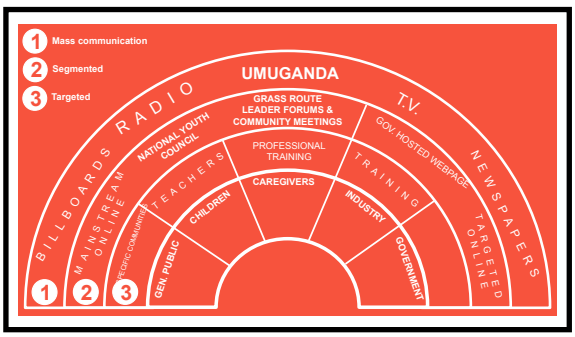
< ПРЕДЫДУЩИЙ РАЗДЕЛ

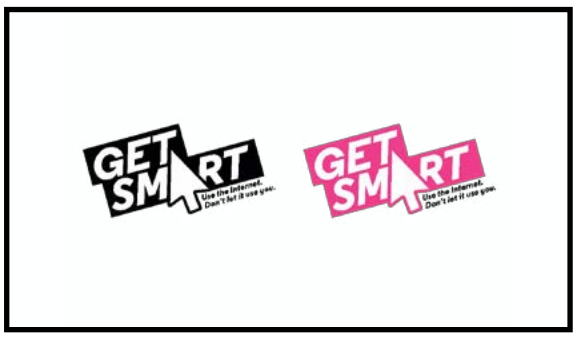
СЛЕДУЮЩИЙ РАЗДЕЛ >

8 Связи с общественностью и формирование коллективной сознательности



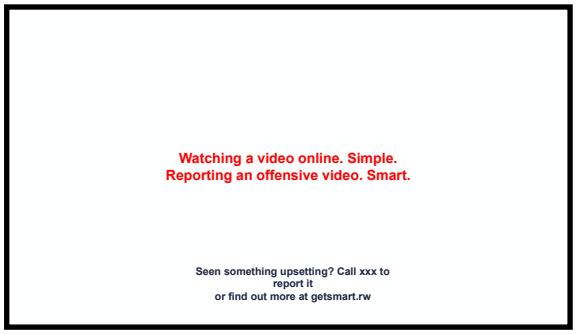






< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

8 Связи с общественностью и формирование коллективной сознательности



2. **Кампания Twisted Toys Фонда 5Rights**[264]
   Кампания, запущенная Фондом 5Rights, повысила осведомленность обо всех видах наблюдения и угроз, с которыми дети могут столкнуться в цифровом мире.

3. **Глобальная неделя медийной и информационной грамотности, ЮНЕСКО**[265]
   Глобальная неделя медийной и информационной грамотности — ежегодное мероприятие, целью которого является анализ прогресса в области достижения общественной медийной и информационной грамотности.

4. **Глобальные рекомендации для родителей, Комиссар по электронной безопасности Австралии**[266]
   В документе, подготовленном Управлением Комиссара по электронной безопасности Австралии, содержатся руководящие указания по защите детей в Интернете для опекунов и родителей.

5. **Справочник для родителей в цифровую эпоху, Совет Европы**[267]
   Справочник, подготовленный Советом Европы, содержит рекомендации по обеспечению безопасности ребенка в Интернете для опекунов и родителей и особенно по защите детей от сексуальной эксплуатации и насилия.

6. **Цели Дня безопасного Интернета в Африке 2021 с талисманом Санго**[268]
   В стремлении построить мир, в котором дети могли бы без ограничений пользоваться всеми преимуществами надежной и безопасной цифровой среды, Международный союз электросвязи определил следующие цели для Африки:

   - ☐ Содействовать образованию и повышению осведомленности о важности безопасности детей в Интернете по всей Африке.
   - ☐ Повысить осведомленность правительств, представителей отрасли, педагогов, детей и родителей, чтобы обеспечить безопасность и защиту африканских детей в Интернете.
   - ☐ Разработать стратегии, направленные на расширение прав и возможностей африканских детей и оказание им поддержки в повышении их устойчивости к угрозам.
   - ☐ Разработать, опубликовать или адаптировать к конкретным условиям имеющиеся ресурсы для обучения и образования детей.

264. Twisted Toys, Фонд 5Rights, 2021 г.
265. Глобальная неделя медийной и информационной грамотности, Организация Объединенных Наций по вопросам образования, науки и культуры, 2021 г.
266. Глобальные рекомендации по безопасности в Интернете для детей и опекунов, Комиссар по электронной безопасности, 2020 г.
267. Родители в цифровую эпоху, Совет Европы, 2017 г.
268. Позиционирование и партнерство по вопросам защиты детей в Интернете, Региональное отделение Международного союза электросвязи (МСЭ) для Африки, 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

8 Связи с общественностью и формирование коллективной сознательности

7. **Тематическое исследование, Министерство информационных технологий и коммуникаций Колумбии**[269]
Министерство информационных технологий и коммуникаций Колумбии содействует развитию цифровых навыков, чтобы уверенно противостоять рискам, связанным с использованием Интернета и ИКТ.

   Целевая аудитория:

   - ☐ дети от 6 до 18 лет;
   - ☐ учащиеся в возрасте от 11 до 28 лет;
   - ☐ взрослые от 28 лет.

   Сайт министерства содержит ссылки на часто задаваемые вопросы, учебные и образовательные ресурсы и доступную информацию о цифровом мире.

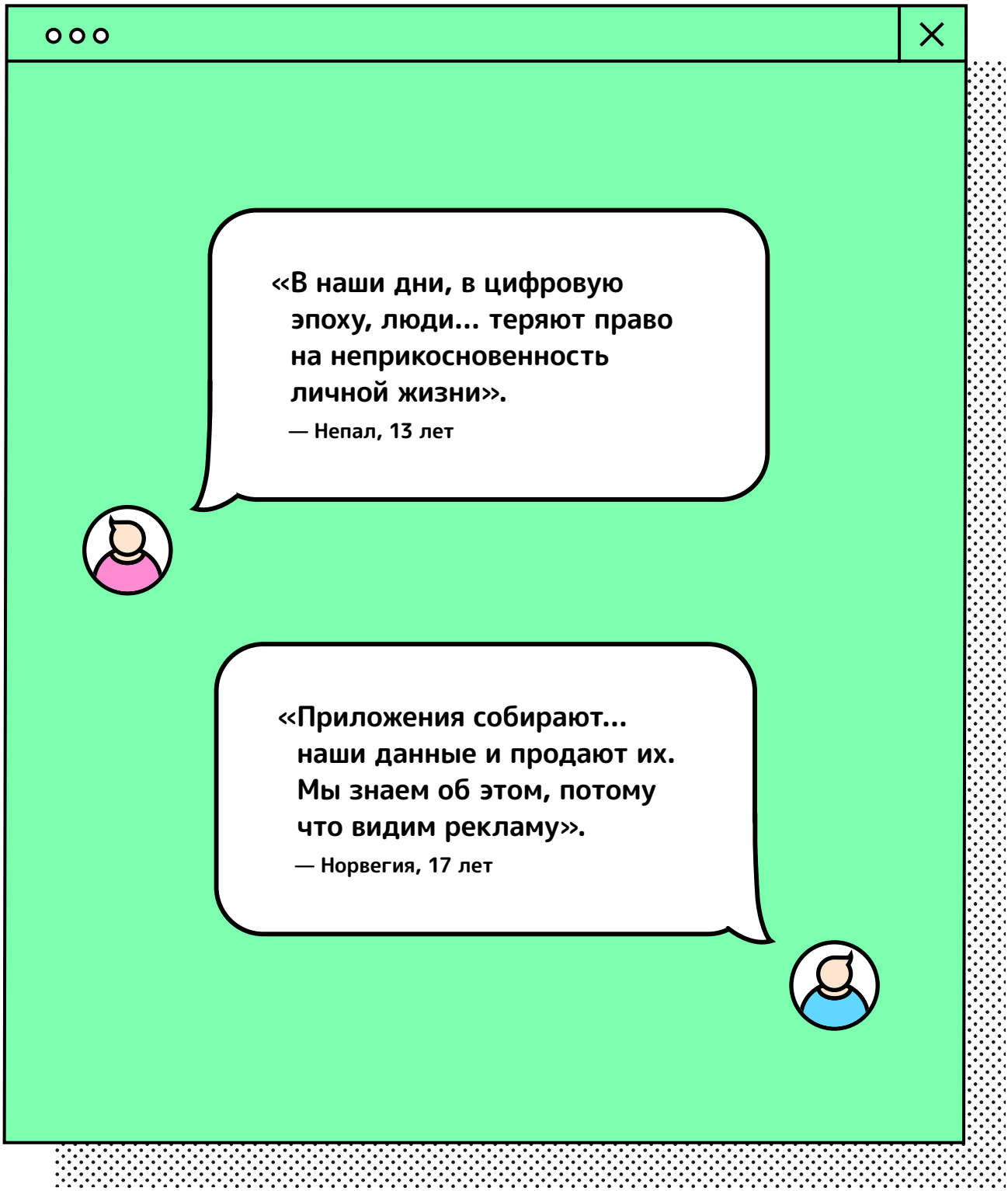
8. **Курс электронного обучения «Меры по прекращению сексуальной эксплуатации детей и жестокому обращению с ними»**[270]
Курс электронного обучения, предназначенный для повышения осведомленности и расширения знаний о сексуальной эксплуатации детей и жестоком обращении с ними, включая насилие, совершаемое с помощью технологий, и для продвижения основанных на фактических данных превентивных и ответных стратегий и мер. Курс охватывает вопросы политики, просветительскую деятельность и широкий круг программных аспектов. Обучающий онлайн-курс и его обзор были подготовлены при финансовой поддержке фонда End Violence.

9. **Как рассказывать о сексуальном насилии над детьми в цифровом мире, Глобальный альянс WeProtect**[271]
В этом стратегическом плане излагаются проблемы, связанные с распространением информации о сексуальной эксплуатации детей и жестоком обращении с ними в Интернете, и предлагаются предварительные рекомендации для специалистов в сфере коммуникаций.

269. En TIC confío+, Министерство информационных технологий и коммуникаций Колумбии, 2021 г.
270. Меры по прекращению сексуальной эксплуатации детей и жестокого обращения с ними, ЮНИСЕФ, 2022 г.
271. Как рассказывать о сексуальном насилии над детьми в цифровом мире, Глобальный альянс WeProtect, 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >



< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

9 Научно-исследовательская работа

> **Регулярное обновление данных и исследования имеют решающее значение для понимания последствий использования цифровых технологий для жизни детей, оценки воздействия на их права и эффективности государственного вмешательства. Странам-участницам следует обеспечить сбор надежных и всеобъемлющих данных из достаточного количества источников, а также их разбивку по возрасту, полу, инвалидности, географическому местоположению, этническим, национальным и социально-экономическим аспектам. Такие данные и исследования, включая те, что проводятся с участием детей и самими детьми, должны служить основой для законодательства, политики и практических мер, а также предаваться гласности. Сбор данных и исследования, касающиеся цифровой жизни детей, должны осуществляться с уважением к их частной жизни и отвечать самым высоким этическим стандартам.**
>
> Источник: Замечание общего порядка № 25 (2021 г.), пункт 30[272]

Цель

Для обеспечения целостного и актуального подхода к безопасности детей в Интернете необходимо выполнить следующие шаги.

Текст типовой политики

Учредить и профинансировать эффективные и общедоступные национальные и региональные научно-исследовательские программы по вопросам безопасности детей в Интернете в целях последующей разработки и осуществления политики в этой области.

9a. Создать программы исследований в области безопасности детей в Интернете
Странам следует учредить центральный научно-исследовательский фонд для разработки научно-исследовательской программы с четко поставленными и актуальными задачами и целями, чтобы обеспечить возможность проведения непрерывных исследований по широкому кругу вопросов безопасности детей в Интернете. Там, где возможно, странам следует поддерживать контакты и сотрудничать друг с другом в области научно-исследовательской работы по вопросам безопасности детей в Интернете. Анализ пробелов призван обеспечить приоритетное выделение ресурсов в областях, в которых ощущается наибольшая потребность, и избежать дублирования исследований. Доступ к исследованиям должен предоставляться региональным или международным партнерам, особенно тем из них, которые располагают наименьшими ресурсами.

9b. Постоянно внедрять инновации
Научные данные будут использоваться при разработке продуктов и услуг со встроенной безопасностью; позволят оценить практическое применение стратегии в отношении безопасности детей в Интернете; а также обеспечат понимание опыта взаимодействия детей с Интернетом и связанных с ним решений в национальном контексте.

9c. Учредить эффективные научно-исследовательские центры по вопросам безопасности детей в Интернете
В рамках существующих учреждений (университетов, медицинских учреждений, центров инноваций) странам следует создать центры передового опыта, которые могли бы обмениваться знаниями об инструментах и услугах, связанных с безопасностью детей в Интернете, и сотрудничать в этой области на национальном, региональном и международном уровнях. ▶

272. Замечание общего порядка № 25 (2021 г.) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

9 Научно-исследовательская работа

9d. Создать четкие этические рамки для научно-исследовательской работы в области безопасности детей в Интернете[273]
Странам следует разработать руководящие принципы для исследователей, занимающихся вопросами безопасности детей в Интернете, включая эффективное включение прав детей в рамки исследовательского процесса. Речь идет о четких инструкциях по сбору данных детей и учете этических и правовых последствий их обработки. Интересы ребенка должны в первую очередь учитываться при создании этических рамок для научно-исследовательской работы по вопросам безопасности детей в Интернете, в том числе в ситуациях, связанных с доступом к информации в общественных интересах.

9e. Создать нормы, регулирующие сбор информации
Регулирующим органам, занимающимся вопросами безопасности детей в Интернете, следует создать механизмы сбора информации, которые позволят им осуществлять мониторинг и оценку эффективности мер по обеспечению безопасности детей в Интернете в различных контекстах и их воздействия на различные группы детей. Мониторинг и оценка мер в этой сфере должны стать частью научно-исследовательской работы.

9f. Обеспечить доступ к данным частных компаний в общественных интересах
Необходимо создать механизмы, в рамках которых социальные сети и другие компании будут делиться своими данными для поддержки исследований с соблюдением наилучших интересов ребенка.

9g. Обеспечить актуальность данных и статистики в конкретных условиях
Для поддержания уровня понимания национальных проблем и адекватного на них реагирования статистические модели должны отражать местную картину и позволять осуществление мониторинга трансграничного воздействия.

273. Дети и жизненный цикл данных: права и этика в мире больших данных, Детский фонд Организации Объединенных Наций, 2017 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

9 Научно-исследовательская работа

План мероприятий для достижения цели

A **Создать программы исследований в области безопасности детей в Интернете**

Странам следует учредить центральный научно-исследовательский фонд для разработки научно-исследовательской программы с четко поставленными и актуальными задачами и целями, чтобы обеспечить возможность проведения непрерывных исследований по широкому кругу вопросов безопасности детей в Интернете. Там, где возможно, странам следует поддерживать контакты и сотрудничать друг с другом в области научно-исследовательской работы по вопросам безопасности детей в Интернете. Анализ пробелов призван обеспечить приоритетное выделение ресурсов в областях, в которых ощущается наибольшая потребность, и избежать дублирования исследований. Доступ к исследованиям должен предоставляться региональным или международным партнерам, особенно тем из них, которые располагают наименьшими ресурсами.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Определить существующие исследовательские фонды и/или учреждения, которые могут проводить или финансировать исследования в области безопасности детей в Интернете.
2. Определить область исследований.
3. Установить строгие критерии в отношении исследований: они должны способствовать повышению грамотности, безопасности и благосостояния детей.
4. Убедиться, что лица, проводящие исследования, осведомлены обо всех областях плана мероприятий, предусмотренного политикой, и не концентрируются исключительно на одной из них.
5. Поставить всё финансирование исследований в зависимость от широкого распространения результатов, включая их хранение в центральном хранилище и предоставление средств на распространение и применение политики.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

9 Научно-исследовательская работа

B **Постоянно внедрять инновации**

Научные данные будут использоваться при разработке продуктов и услуг со встроенной безопасностью; позволят оценить практическое применение стратегии в отношении безопасности детей в Интернете; а также обеспечат понимание опыта взаимодействия детей с Интернетом в национальном контексте.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Отслеживать изменения (в глобальном масштабе) в отношении продуктов и услуг и их широкое распространение, чтобы достижения в области безопасности детей в одной части мира были доступны для других стран.
2. Отслеживать области, в которых были достигнуты успехи, и привлекать к их распространению международные НПО или экспертные группы.
3. Заключить с межправительственными организациями, частными компаниями и НПО соглашения по распространения передовой практики. Например, безвозмездная передача компьютерного оборудования должна осуществляться только при условии включения функций безопасности и конфиденциальности по умолчанию.

C **Учредить эффективные научно-исследовательские центры по вопросам безопасности детей в Интернете**[274]

Странам следует учредить специализированные центры, которые могли бы обмениваться знаниями и сотрудничать в области разработки инструментов, услуг и навыков, связанных с безопасностью детей в Интернете, на национальном, региональном и международном уровнях.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Учредить центры по вопросам безопасности детей в Интернете в существующих государственных ведомствах или учебных заведениях.
2. Рассмотреть возможность создания центров по вопросам безопасности детей в Интернете в регионах с аналогичными культурными и организационными условиями для обмена передовым опытом.

274. Безопасность детей в Интернете: глобальные проблемы и стратегии, Детский фонд Организации Объединенных Наций, 2011 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

9 Научно-исследовательская работа

D **Создать четкие этические рамки для научно-исследовательской работы в области безопасности детей в Интернете**[275]

Странам следует разработать руководящие принципы для исследователей, занимающихся вопросами безопасности детей в Интернете, включая эффективное включение прав детей в рамки исследовательского процесса. Речь идет о четких инструкциях по сбору данных детей и учете этических и правовых последствий их обработки. Интересы ребенка должны в первую очередь учитываться при создании этических рамок для научно-исследовательской работы по вопросам безопасности детей в Интернете, в том числе в ситуациях, связанных с доступом к информации в общественных интересах.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Установить минимальные стандарты ответственного исследования (см., в частности, Руководящие принципы ECPAT в разделе «Ресурсы» ниже).
2. Обеспечить, чтобы соблюдение стандартов являлось условием финансирования и/или принятия результатов исследований. См. Средство поддержки 1 (стр. 156).
3. Обеспечить обязательное обучение исследователей по вопросам безопасности детей (см. пункт «Обучение» раздела «Область применения политики», стр. 144).

E **Создать нормы, регулирующие сбор информации**

Регулирующим органам, занимающимся вопросами безопасности детей в Интернете, следует создать механизмы сбора информации, которые позволят им осуществлять мониторинг и оценку эффективности мер по обеспечению безопасности детей в Интернете в различных контекстах и их воздействия на различные группы детей. Мониторинг и оценка мер в этой сфере должны стать частью научно-исследовательской работы.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, необходимо обеспечить, чтобы регулирующие органы требовали использования механизма сбора информации для понимания ресурсов, методов и результатов. Любые правовые или нормативные требования должны включать полномочия по отчетности, прозрачности и сбору информации. в качестве примеров можно привести GDPR[276] и законопроект Великобритании о безопасности в Интернете.[277]

275. Дети и жизненный цикл данных: права и этика в мире больших данных, Детский фонд Организации Объединенных Наций, 2017 г.
276. Общий регламент о защите данных, Европейский союз, 2018 г.
277. Законопроект о безопасности в Интернете, Департамент цифровых технологий, культуры и средств массовой информации, 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

9 Научно-исследовательская работа

F **Обеспечить доступ к данным частных компаний в общественных интересах**

Необходимо создать механизмы, в рамках которых социальные сети и другие компании будут делиться своими данными для поддержки исследований с соблюдением наилучших интересов ребенка.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Проводить работу с компаниями социальных сетей на соответствующей территории, запрашивая доступ к наборам данных, где это уместно.
2. Присоединяться к региональным, национальным или глобальным инициативам, делающим похожие запросы.

G **Обеспечить актуальность данных и статистики в конкретных условиях**

Регулирующие органы, работающие в области безопасности детей в Интернете, должны создать механизмы для сбора информации, которые позволят им контролировать и оценивать эффективность мер обеспечения безопасности детей в Интернете в различных контекстах, а также их воздействие на различные группы детей. Мониторинг и оценка мер по обеспечению безопасности детей в Интернете должны стать частью научно-исследовательской работы.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Найти документально подтвержденные статистические данные из авторитетных источников.
2. Провести совместную работу с заинтересованными сторонами таких ведомств, чтобы проверить и подтвердить имеющуюся в распоряжении статистику.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

9 Научно-исследовательская работа

Как это согласуется с основополагающими документами

Возможность 2 Модель национального реагирования. Исследование, анализ и мониторинг передовой практики правоохранительной деятельности:

Как минимум, целями анализа должны являться следующие: оценка существующей угрозы сексуальной эксплуатации детей и жестокого обращения с ними (CSEA), того, как она проявляется и кто подвергается наибольшему риску; оценка уязвимости страны к этой угрозе; оценка существующих институциональных мер реагирования; мониторинг применения законодательства и политики для оценки его соответствия международным стандартам и передовой практике; пересмотр текущих мер реагирования на экосистемы ИКТ, включая механизмы сообщения о нарушениях с помощью горячей линии и отраслевого участия; а также отслеживание деятельности других заинтересованных сторон, занимающихся этим вопросом.

Для обоснования анализа необходимо обеспечить доступ к широкому кругу актуальных данных и информации о сексуальной эксплуатации детей и жестоком обращении с ними (CSEA) от национальных организаций и любых других связанных с вопросом заинтересованных сторон. Кроме того, первичные данные должны собираться из различных источников, таких как дети, родители, преподаватели, сотрудники правоохранительных органов и поставщики услуг.

Источник: Модель национального реагирования Глобального альянса WeProtect, стр. 5–6[278]

278. Модель национального реагирования, Глобальный альянс WeProtect, 2016 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

9 Научно-исследовательская работа

Средства поддержки

1. Контрольный список этических аспектов исследования

Цель D («Создать четкие этические рамки для научно-исследовательской работы в области безопасности детей в Интернете») подчеркивает необходимость целостного подхода к этике исследований на уровнях методологии, финансирования и сбора данных. Данный контрольный список призван помочь в создании учитывающих перечисленные аспекты этических рамок.

Учитывается ли в наборе исследований, выбранных для государственного финансирования, вопрос безопасности детей в Интернете?

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, как будет решаться эта проблема?

Включает ли финансирование исследований оценку их воздействия на права детей или этическую экспертизу?

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, как будет решаться эта проблема?

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

9 Научно-исследовательская работа

Существуют ли этические рамки для исследователей и разработчиков, включающие аспекты прав детей?

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, как будет решаться эта проблема?

Прошли ли исследователи, разработчики и лица, принимающие решения по финансированию, обучение по вопросам безопасности детей в Интернете и прав ребенка?

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, как будет решаться эта проблема?

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

9 Научно-исследовательская работа

Применяется ли принцип предотвращения к научно-исследовательской работе?

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, как будет решаться эта проблема?

Доступны ли данные из открытых источников для поддержки исследований в области безопасности детей в Интернете?

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, как будет решаться эта проблема?

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

9 Научно-исследовательская работа

Прочие справочные ресурсы

1. **Нормативно-правовое регулирование ответственных исследований и инноваций в области ИКТ, Оксфордский университет**[279]
   Данный документ, разработанный при финансировании Научно-исследовательского совета по инженерным и физическим наукам (EPSRC), посвящен этическим аспектам исследований в области ИКТ. Он был подготовлен Центром ответственных исследований и инноваций в области ИКТ (ORBIT) с целью предоставить четкие инструкции о том, как проводить практические и этические исследования.

2. **Предотвращение нарушений, партнерство End Violence**[280]
   Документ, созданный в партнерстве с ECPAT International, ИНТЕРПОЛОМ, Управлением исследований ЮНИСЕФ при финансовой поддержке партнерства End Violence, — это исследовательский проект, дающий представление о том, каким образом цифровые технологии способствуют сексуальной эксплуатации детей и жестокому обращению с ними в 13 странах Восточной и Южной Африки, а также Юго-Восточной Азии.

3. **Руководящие принципы этических исследований в области сексуальной эксплуатации детей, ECPAT**[281]
   Руководство, предназначенное для тех, кто проводит исследования по вопросам, связанным с сексуальной эксплуатацией детей и жестоким обращением с ними, помогает разрешить возникающие в связи с этим этические вопросы и дилеммы. Эти руководящие принципы помогают исследователям оформить свой проект таким образом, чтобы свести к минимуму вред для детей.

4. **Мнение Агентство Европейского Союза по основным правам**[282]
   Мнение 9 Агентства ЕС по основным правам: всякий раз, когда ЕС и его страны-участницы финансируют научно-исследовательскую работу, они должны требовать от подрядчиков привлекать к ним экспертов по защите персональных данных и других основных прав. Научные исследователи и представители отрасли должны включать в тестовые группы людей с разными фенотипическими характеристиками, различного возраста и гендера, чтобы исключить любые риски дискриминационных результатов.

5. **Руководящие принципы правозащитного подхода к данным, Управление Верховного комиссара ООН по правам человека**[283]
   В данном руководстве содержатся рекомендации и принципы в отношении совершенствования методов использования данных и статистики для заинтересованных сторон и законодателей. Оно обеспечивает соблюдение, защиту и осуществление прав человека с опорой на Повестку дня на период до 2030 года при сборе или дезагрегировании данных.

279. Нормативно-правовое регулирование ответственных исследований и инноваций в области ИКТ, Оксфордский университет, 2014 г.
280. Предотвращение нарушений, партнерство End Violence, 2019 г.
281. Руководящие принципы этических исследований в области сексуальной эксплуатации детей, ECPAT International, 2019 г.
282. Под наблюдением: биометрические данные. Системы ИТ и основные права в ЕС, Агентство Европейского Союза по основным правам, 2018 г.
283. Правозащитный подход к данным, Управление Верховного комиссара Организации Объединенных Наций по правам человека, 2018 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

«В наши дни цифровые технологии облегчают незаконный доступ к данным и конфиденциальной информации без согласия людей».

— Пакистан, 12 лет

«Зачем [сайтам и социальным сетям] запрашивать у меня личную информацию, если они не используют ее в каких-либо целях?»

— Объединенные Арабские Эмираты, 17 лет

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

10 Международное сотрудничество

Трансграничный и транснациональный характер цифровой среды требует активного международного и регионального сотрудничества для обеспечения того, чтобы все заинтересованные стороны, включая государства, предприятия и другие субъекты, эффективно соблюдали, защищали и осуществляли права детей в Интернете. Поэтому крайне важно, чтобы страны-участницы сотрудничали на двусторонней и многосторонней основе с национальными и международными неправительственными организациями, ведомствами Организации Объединенных Наций, бизнесом и организациями, специализирующимися на защите детей и человека в цифровой среде.

Странам-участницам следует поощрять международный и региональный обмен опытом и передовой практикой, вносить свой вклад в этот процесс, а также создавать и поддерживать развитие потенциала, ресурсы, стандарты, нормативные положения и меры защиты за пределами национальных границ, что позволит всем государствам осуществлять права детей в цифровой среде. Они должны поощрять разработку общего определения преступления в цифровой среде, взаимную правовую помощь и совместный сбор доказательств и обмен ими.

Источник: Замечание общего порядка № 25 (2021 г.), пункты 123 и 124[284]

Цель

Сотрудничать с национальными, региональными и глобальными организациями и другими заинтересованными сторонами для обмена передовым опытом.

Текст типовой политики

Для обеспечения целостного подхода к безопасности детей в Интернете необходимо предпринять следующие шаги.

10a. Установить официальные рамки взаимодействия (например, заключить меморандумы о взаимопонимании) с региональными и глобальными сообществами по безопасности детей в Интернете
Укрепление международного сотрудничества в целях повышения безопасности детей в Интернете во всем мире имеет решающее значение для обеспечения глобальной безопасности. Странам следует официально закрепить сотрудничество для совместных государственно-частных инвестиций в областях, связанных, в частности, с кибербезопасностью, наращиванием потенциала для обеспечения безопасности детей в Интернете, инновациями, правоохранительной деятельностью, системой правосудия, образовательными программами и т. д.

10b. Стать участником региональных и международных правовых инструментов, поощряющих сотрудничество по вопросам безопасности детей в Интернете
Странам следует определить ключевые региональные и международные инструменты, которые позволят им сотрудничать с другими странами в вопросах обеспечения безопасности детей в Интернете. в частности, речь идет о международных соглашениях о сотрудничестве между правоохранительными органами; международной передовой практике; международных программах, которые могут обеспечить ресурсы для сотрудничества по вопросам безопасности детей в Интернете; а также доступе ко всем правам человека или связанным с ними стандартам, которые будут способствовать сотрудничеству между странами. ▶

284. Замечание общего порядка № 25 (2021 год) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

10 Международное сотрудничество

10c. Определить страны и организации, которые могут предоставить соответствующие модели и поддержку для повышения безопасности детей в Интернете
В некоторых случаях нет необходимости разрабатывать политику с нуля. Странам следует найти полезные примеры концепций обеспечения безопасности детей в Интернете, которые могут быть использованы и адаптированы к конкретным условиям. Обмен информацией о проблемах и трудностях, связанных с безопасностью детей в Интернете, может быть весьма полезным для планирования, разработки и осуществления политики.

10d. Поддерживать другие страны, разрабатывающие политику безопасности детей в Интернете
По возможности, важно делиться информацией о типовых законах, нормативных рамках, извлеченных уроках и прочими материалами, которые могут быть использованы другими странами для разработки собственной концепции и политики в области безопасности детей в Интернете.[285]

План мероприятий для достижения цели

A **Установить официальные рамки взаимодействия (например, заключить меморандумы о взаимопонимании) с региональными и глобальными сообществами по безопасности детей в Интернете**

Укрепление международного сотрудничества в целях повышения безопасности детей в Интернете во всем мире имеет решающее значение для обеспечения глобальной безопасности. Странам следует официально закрепить сотрудничество для совместных государственно-частных инвестиций в областях, связанных, в частности, с кибербезопасностью, наращиванием потенциала для обеспечения безопасности детей в Интернете, инновациями, правоохранительной деятельностью, системой правосудия, образования и т. д.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Определить соответствующие региональные и глобальные соглашения и договоры в области безопасности детей в Интернете (см. раздел «Основные документы»).
2. Начать официально использовать и добавить необходимые меры в план мероприятий по повышению безопасности детей в Интернете.
3. Убедиться, что они, как минимум, включают в себя любые меры, определенные в следующих документах:

- ☐ Цели в области устойчивого развития[286]
- ☐ Конвенция о правах ребенка и факультативные протоколы к ней[287]
- ☐ Замечание общего порядка № 25 (2021 г.) о правах детей в отношении цифровой среды.[288]
- ☐ Модель национального реагирования.[289] См. Средство поддержки 1 (стр. 166).

285. См., например, материалы по международному лидерству и сотрудничеству, подготовленные комиссаром по электронной безопасности Австралии, 2021 г.
286. Преобразование нашего мира: Повестка дня в области устойчивого развития на период до 2030 года, Организация Объединенных Наций, 2021 г.
287. Конвенция о правах ребенка, Управление Верховного комиссара Организации Объединенных Наций по правам человека, 1989 г.
288. Замечание общего порядка № 25 (2021 г.) о правах детей в отношении цифровой среды, Комитет Организации Объединенных Наций по правам ребенка, 2021 г.
289. Модель национального реагирования, WeProtect, 2016 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

10 Международное сотрудничество

B **Стать участником региональных и международных правовых инструментов, поощряющих сотрудничество по вопросам безопасности детей в Интернете**

Странам следует определить ключевые региональные и международные инструменты, которые позволят им сотрудничать с другими странами в вопросах обеспечения безопасности детей в Интернете. в частности, речь идет о международных соглашениях о сотрудничестве между правоохранительными органами; международной передовой практике; международных программах, которые могут обеспечить ресурсы для сотрудничества по вопросам безопасности детей в Интернете; а также доступе ко всем правам человека или связанным с ними стандартам, которые будут способствовать сотрудничеству между странами.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Обратиться в международные правоохранительные органы, такие как ИНТЕРПОЛ[290] и Европол.[291]
2. Обратиться к передовому опыту глобальных организаций, таких как Национальный центр по делам пропавших без вести и эксплуатируемых детей[292] и Internet Watch Foundation.[293]

290. Кто мы, ИНТЕРПОЛ.
291. О Европоле, Европол.
292. Наша работа, Национальный центр по делам пропавших и эксплуатируемых детей (NCMEC).
293. О нас, Internet Watch Foundation (IWF).

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

10 Международное сотрудничество

C **Определить страны и организации, которые могут предоставить соответствующие модели и поддержку для повышения безопасности детей в Интернете**

В некоторых случаях нет необходимости разрабатывать политику с нуля. Странам следует найти полезные примеры концепций обеспечения безопасности детей в Интернете, которые могут быть использованы и адаптированы к конкретным условиям. Обмен информацией о проблемах и трудностях, связанных с безопасностью детей в Интернете, может быть весьма полезным для планирования, разработки и осуществления политики.

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, можно обратиться в региональные органы, такие как Азиатская коалиция по правам ребенка[294], к национальным лидерам, таким как Alana Foundation в Бразилии[295], или в экспертные организации, такие как Internet Watch Foundation[296], Фонд 5Rights[297], ЮНИСЕФ[298], INHOPE[299] или инициатива «Безопасность в Интернете» (Safe Online) Глобального партнерства по борьбе с насилием в отношении детей.[300]Вышеперечисленные организации располагают необходимыми ресурсами и информацией и во многих случаях способны помочь в определении местных и полезных партнерств.

294. О нас, Азиатская коалиция по правам ребенка.
295. О нас, Alana Foundation.
296. О нас, Internet Watch Foundation (IWF).
297. Фонд 5Rights, Фонд 5Rights.
298. О нас, ЮНИСЕФ.
299. Наша история, INHOPE, 2021 г.
300. «Безопасность в Интернете», Глобальное партнерство по борьбе с насилием над детьми, 2022 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

10 Международное сотрудничество

D **Поддерживать другие страны, разрабатывающие политику безопасности детей в Интернете**

По возможности, важно делиться информацией о типовых законах, нормативных рамках, извлеченных уроках и прочими материалами, которые могут быть использованы другими странами для разработки собственной концепции и политики в области безопасности детей в Интернете.[301]

Если эти шаги выполнены, предоставьте подробную информацию:

Если нет, может быть полезно:

1. Определить другие организации и/или ведущие министерства в вашем регионе.
2. Рассмотреть передовой опыт других регионов, например Ассоциации государств Юго-Восточной Азии (АСЕАН) или ЕС.
3. Поделиться своими ресурсами и решениями.
4. Подумать, как установить партнерские отношения с теми, у кого меньше ресурсов.
5. Поощрять получателей помощи делиться ей с другими.
6. Учитывать передовые международные практики и в инициативном порядке делиться опытом со странами, которые располагают меньшими ресурсами, или помогать им иным образом: например, налаживать двусторонние связи с конкретной страной или регионом, предоставлять ей (ему) техническую поддержку, включая юридическую или языковую, включая перевод отдельных частей плана мероприятий, либо проводить семинары для рядовых работников, в том числе работников правоохранительных органов.

Как это согласуется с основополагающими документами

Рекомендуем Генеральному секретарю ООН в срочном порядке обеспечить гибкий и открытый процесс консультаций для разработки обновленных механизмов глобального цифрового сотрудничества. в качестве отправной точки можно воспользоваться вариантами, описанными в главе 4. в качестве первоначальной цели предлагаем включить в мероприятие по поводу 75-летия ООН в 2020 г. «Глобальное обязательство по цифровому сотрудничеству», чтобы закрепить общие ценности, принципы, понимание и цели для улучшения глобальной архитектуры цифрового сотрудничества. в рамках этого процесса Генеральный секретарь Организации Объединенных Наций может назначить посланника по делам технологий.

5B: Мы поддерживаем многосторонний «системный» подход к сотрудничеству и регулированию, который является адаптивным, гибким, инклюзивным и подходящим для целей цифрового века.

Источник: Эпоха цифровой взаимозависимости, Группа высокого уровня Генерального секретаря ООН по цифровому сотрудничеству, 2019 г.[302]

301. См., например, материалы по международному лидерству и сотрудничеству, подготовленные комиссаром по электронной безопасности Австралии.
302. Эпоха цифровой взаимозависимости, Группа высокого уровня Генерального секретаря ООН по цифровому сотрудничеству, 2019 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

10 Международное сотрудничество

Средства поддержки

1. Контрольный список требований международных рамочных систем

Цель a («Установить официальные рамки взаимодействия (например, заключить меморандумы о взаимопонимании) с региональными и глобальными сообществами по безопасности детей в Интернете») предусматривает соблюдение минимальных требований, содержащихся в ряде международных протоколов и передовых документов. Ведущим министерствам совместно с правительством следует использовать этот инструмент для оценки соответствия таким требованиям.

	Опишите, как выполняются минимальные требования	**Пробелы в соответствии требованиям**	**Дата уведомления об этих пробелах ведущего министерства**	**Дата уведомления об этих пробелах группы заинтересованных сторон по вопросам безопасности детей в Интернете**
Цели ООН в области устойчивого развития				
Конвенция ООН о правах ребенка				
Факультативный протокол КПР, касающийся участия детей в вооруженных конфликтах				
Торговля детьми, детская проституция и детская порнография				
Процедура сообщений				

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

10 Международное сотрудничество

	Опишите, как выполняются минимальные требования	Пробелы в соответствии требованиям	Дата уведомления об этих пробелах ведущего министерства	Дата уведомления об этих пробелах группы заинтересованных сторон по вопросам безопасности ребенка в Интернете
Замечание общего порядка № 25 (2021 г.)	☑			
Модель национального реагирования				
Люксембургские руководящие принципы терминологии для защиты детей от сексуальной эксплуатации и сексуальных надругательств				

Прочие справочные ресурсы

Нормативные документы в поддержку международного сотрудничества

1. **План мероприятий ООН по цифровому сотрудничеству**[303]
   В 2020 году был опубликован План мероприятий по цифровому сотрудничеству[304], подготовленный Генеральным секретарем при поддержке Группы высокого уровня по вопросам цифрового сотрудничества. в нем содержатся рекомендации для различных заинтересованных сторон по укреплению глобального сотрудничества в области цифровых технологий.

2. **ВЕБ-РЕСУРС ИНТЕРПОЛА о преступлениях против детей**[305]
   На сайте ИНТЕРПОЛА размещен широкий спектр ресурсов, включая информацию о работе ИНТЕРПОЛА, а также сведения о базе данных по сексуальной эксплуатации детей и жестокому обращении с ними (CSEA) в Интернете, блокировании и категоризации контента, а также выявлении жертв.

3. **Рекомендация Совета ОЭСР по защите детей в Интернете**[306]
   В рекомендациях излагаются принципы и руководящие указания, призванные помочь странам найти баланс между защитой детей от рисков в Интернете и использованием возможностей и преимуществ, предоставляемых цифровым миром.

303. План мероприятий Генерального секретаря Организации Объединенных Наций по цифровому сотрудничеству, Организация Объединенных Наций, 2020 г.
304. Группа высокого уровня Генерального секретаря Организации Объединенных Наций по цифровому сотрудничеству, Организация Объединенных Наций, 2020 г.
305. Преступления против детей, ИНТЕРПОЛ.
306. Рекомендации по защите детей в Интернете, ОЭСР, принятые в 2012 году с поправками 2021 года.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

10 Международное сотрудничество

Прочие справочные ресурсы

Нормативные документы в поддержку регионального сотрудничества

1. **Конвенция Африканского союза о кибербезопасности и защите персональных данных, Малабо, 2014 г.**[307]
   Конвенция Африканского союза направлена на создание «надежной концепции для кибербезопасности в Африке посредством организации электронных транзакций, защиты персональных данных, продвижения кибербезопасности, электронного управления и борьбы с киберпреступностью».

2. **Повестка дня Африканского союза в области защиты детей на период до 2040 года**[308]
   Повестка дня Африканского союза на период до 2040 года (Повестка дня на период до 2063 года) содержит цели по защите детей на всем континенте. Она основывается на пункте 53, в котором утверждается, что «африканские дети должны быть наделены правами и возможностями посредством полного осуществления Африканской хартии прав и благополучия ребенка».

3. **Стратегия Европейской комиссии по улучшению Интернета для детей**[309]
   В стратегии Европейской комиссии по улучшению Интернета рассматриваются цифровые навыки и инструменты для детей, а также описывается потенциал рынка для разработки интерактивного, творческого и образовательного цифрового контента.

4. **Модель национального реагирования Глобального альянса WeProtect (MNR)**[310]
   Модель национального реагирования (MNR) направлена на оказание помощи странам в разработке мер реагирования на сексуальную эксплуатацию детей и жестокое обращение с ними в Интернете, однако в ней также подчеркивается, что эту проблему невозможно решить изолированно. Для обеспечения комплексных мер национального реагирования необходим более широкий набор возможностей по предотвращению этой проблемы и борьбе с ней.

5. **Карта политики «Улучшение Интернета для детей» (BIK)**[311]
   Карта политики «Улучшение Интернета для детей» (BIK) предоставляет полный обзор стратегий и политики в области улучшения Интернета для детей, в настоящее время реализуемых во всех странах-участницах ЕС.

6. **Региональный план действий АСЕАН по искоренению насилия в отношении детей**[312] **и Декларация АСЕАН о защите детей от всех форм эксплуатации и жестокого обращения в Интернете**[313]
   Региональный план представляет собой план мероприятий, призванный помочь странам-участницам в осуществлении декларации АСЕАН 2013 года о защите детей от всех форм эксплуатации в Интернете. ▶

307. Конвенция Африканского союза о кибербезопасности и защите персональных данных, Африканский союз, 2014 г.
308. Африканская повестка дня по защите детей на период до 2040 года, Fostering an Africa Fit for Children, Африканский комитет экспертов по правам и благополучию детей, 2016 г.
309. Европейская стратегия по улучшению Интернета для детей, Европейская комиссия, 2021 г.
310. Модель национального реагирования, Глобальный альянс WeProtect, 2016 г.
311. Карта политики «Улучшение Интернета для детей», Better Internet for Kids, 2020 г.
312. Региональный план действий АСЕАН по искоренению насилия в отношении детей, Детский фонд Организации Объединенных Наций, 2019 г.
313. Прекращение насилия в отношении детей в государствах-членах АСЕАН, Отделение ЮНИСЕФ в Восточной Азии и Тихом океане, 2019 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

7. **Тематическое исследование, Конвенция Совета Европы**
   Конвенция Совета Европы по защите детей от сексуальной эксплуатации и надругательств сексуального характера, также известная как «Конвенция Лансароте»»[314], требует криминализации всех видов сексуальных преступлений в отношении детей. в ней говорится, что государства в Европе и за ее пределами должны принять конкретные законы и меры для предотвращения сексуального насилия, защиты детей-жертв и судебного преследования виновных.

   «Комитет Лансароте»»[315](Комитет Сторон Конвенции Лансароте) — орган, созданный для контроля за тем[316], насколько эффективно Стороны осуществляют Конвенцию Лансароте. Комитету также поручено выявлять передовую практику[317], в частности в ходе деятельности по наращиванию потенциала[318] (визиты исследования, конференции и т. д.).

   Совет Европы помогает защитить общество во всем мире от угрозы киберпреступности с помощью Будапештской конвенции по борьбе с киберпреступностью и прилагаемого к ней Протокола о ксенофобии и расизме, Комитета Конвенции о киберпреступности (ККИ) и программ технического сотрудничества в области киберпреступности.

   Конвенция является первым международным соглашением в отношении преступлений, совершаемых в Интернете и других компьютерных сетях и касающихся, в частности, нарушения авторского права, мошенничества с использованием компьютерных сетей, детской порнографии и нарушений безопасности сети. Она также предусматривает ряд полномочий и процедур, таких как поиск компьютерных сетей и перехват электронных сообщений.

8. **Принципы и рекомендации Организации американских государств по защите данных (Защита персональных данных)[319]**
   Документ стал результатом исследования стандартов по защите данных, проведенного Межамериканским юридическим комитетом. Принципы представляют собой модель доступа к общественной информации для межамериканского законодательства. Они содержат руководство Генерального секретариата по оказанию поддержки странам-участницам в разработке, осуществлении и оценке местных правовых рамок, касающихся доступа к общественной информации.

Нормативные документы в поддержку межстранового сотрудничества и партнерств

9. **Люксембургские руководящие принципы терминологии для защиты детей от сексуальной эксплуатации и сексуальных надругательств[320]**
   Эти руководящие принципы представляют собой инициативу 18 международных партнеров по согласованию терминов и определений, касающихся защиты детей. Они направлены на повышение концептуальной ясности терминологии с тем, чтобы обеспечить более решительную и последовательную просветительскую деятельность, политику и законы на всех языках во всех регионах мира.

10. **Поддержка разработки руандской политики в отношении безопасности детей в Интернете со стороны полиции Шотландии[321]**
    Речь идет о партнерстве между полицией Шотландии и правительством Руанды. Его подробное описание приведено в публикации блога Фонда 5Rights.

314. Конвенция Лансароте, Совет Европы.
315. Комитет Лансароте, Совет Европы.
316. Контроль за осуществлением Конвенции Лансароте, Совет Европы.
317. Положительный опыт осуществления Конвенции Лансароте, Совет Европы.
318. Конвенция Лансароте, Совет Европы.
319. Принципы и рекомендации по защите данных, Постоянный совет Организации американских государств, 2011 г.
320. Люксембургские руководящие принципы, ECPAT, 2016 г.
321. Поддержка безопасности детей в Интернете в сотрудничестве с правительством Руанды и полицией Шотландии, Фонд 5Rights, 2020 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

11. **Всеобщая декларация «Безопасность детей в Интернете»**[322]
    Декларация Комиссии по широкополосной связи, цель которой — донести важность общей миссии по защите детей в Интернете до всех заинтересованных сторон.

Примеры сотрудничества между правоохранительными органами[323]

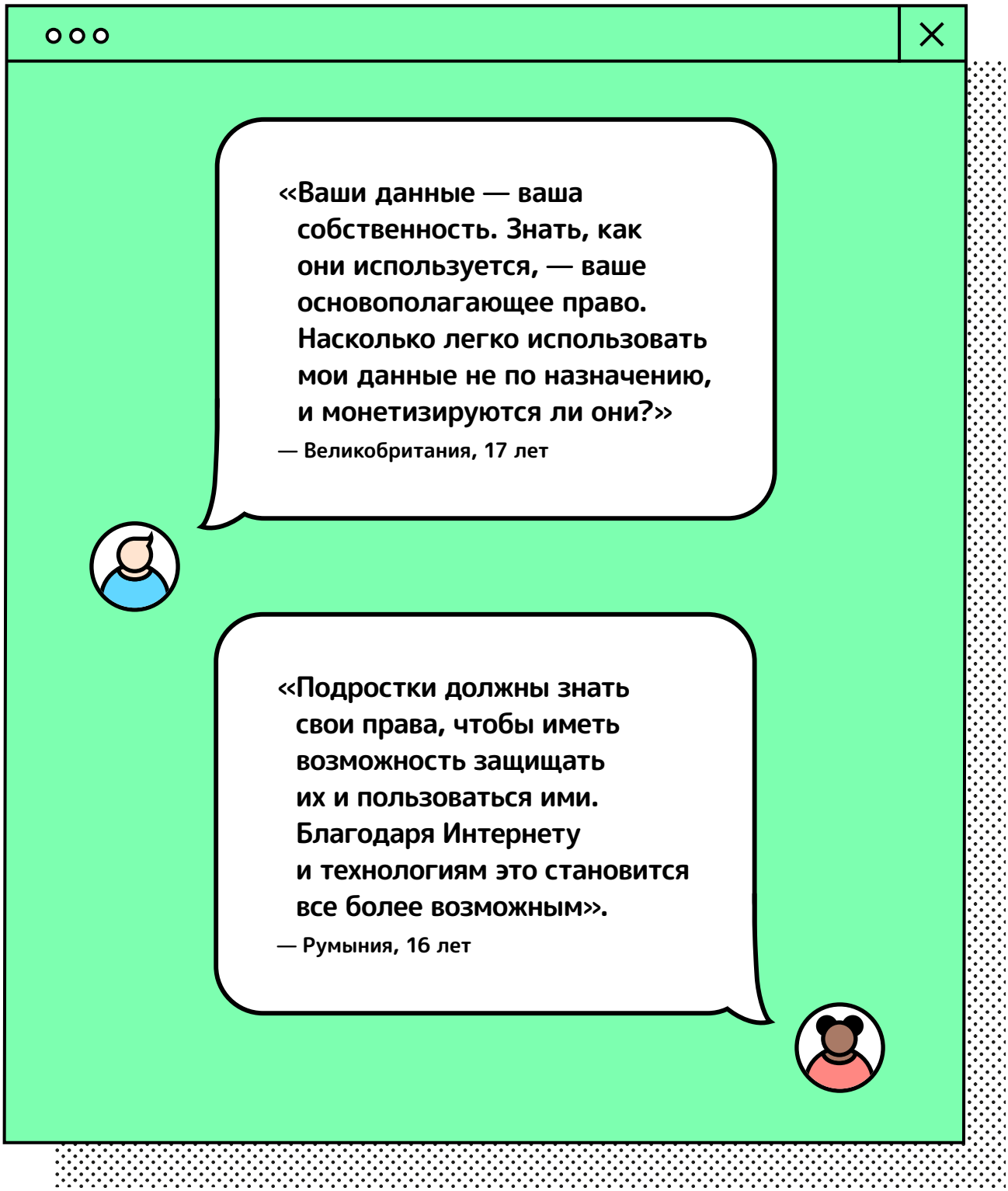
12. **Виртуальная глобальная целевая группа**[324]
    Данная целевая группа представляет национальные, региональные и международные правоохранительные органы со всего мира, объединившиеся для борьбы с сексуальными насилием над детьми в Интернете. Она также обеспечивает связь с региональными службами охраны правопорядка и горячими линиями по вопросам сексуальной эксплуатации детей и жестокого обращения с ними, по которым поступают сообщения.

13. **Руководство Совета Европы по сотрудничеству между правоохранительными органами и интернет-провайдерами в борьбе с киберпреступностью**[325]
    Настоящий документ представляет собой свод руководящих принципов, разработанных для оказания помощи поставщикам услуг и правоохранительным органам в любой стране в налаживании эффективного сотрудничества. Он доступен более чем на десяти языках.

322. Всеобщая декларация «Безопасность детей в Интернете», Комиссия по широкополосной связи, 2019 г.
323. Уведомление и удаление: политика и практика компаний по удалению материалов по сексуальным надругательствам над детьми в Интернете, Детский фонд Организации Объединенных Наций и GSMA, 2016 г.
324. Виртуальная глобальная целевая группа, Виртуальная глобальная целевая группа, 2016 г.
325. Руководящие принципы сотрудничества между правоохранительными органами и интернет-провайдерами, Совет Европы, 2007 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >



«Ваши данные — ваша собственность. Знать, как они используется, — ваше основополагающее право. Насколько легко использовать мои данные не по назначению, и монетизируются ли они?»

— Великобритания, 17 лет

«Подростки должны знать свои права, чтобы иметь возможность защищать их и пользоваться ими. Благодаря Интернету и технологиям это становится все более возможным».

— Румыния, 16 лет

СИСТЕМНАЯ ПАПКА

8 ДОКУМЕНТОВ | 105 МБ НА ДИСКЕ | РАЗДЕЛ 6

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

Основные документы

Конвенция ООН о правах ребенка и связанные с ней документы:

1. **Конвенция ООН о правах ребенка**[326]
   Принята и открыта для подписания, ратификации и присоединения резолюцией 44/25 Генеральной Ассамблеи от 20 ноября 1989 г.; вступила в силу 2 сентября 1990 г. в соответствии со статьей 49.

   Существует также адаптированная для детей текстово-графическая версия Конвенции о правах ребенка (см. также раздел «Важность соблюдения прав детей»), призванная помочь детям понять свои права.

2. **Факультативный протокол к Конвенции о правах ребенка, касающийся торговли детьми, детской проституции и детской порнографии**[327]
   Принят и открыт для подписания, ратификации и присоединения резолюцией A/RES/54/263 Генеральной Ассамблеи от 25 мая 2000 г.; вступил в силу 18 января 2002 г.

3. **Факультативный протокол к Конвенции о правах ребенка, касающийся участия детей в вооруженных конфликтах**[328]
   Принят и открыт для подписания, ратификации и присоединения резолюцией A/RES/54/263 Генеральной Ассамблеи от 25 мая 2000 г.; вступил в силу 12 февраля 2002 г.

4. **Факультативный протокол к Конвенции о правах ребенка, касающийся процедуры сообщений32**[9]
   Резолюция, принятая Генеральной Ассамблеей 19 декабря 2011 г.

5. **Руководство ЮНИСЕФ. Как Конвенция ООН о правах ребенка защищает права детей**[330]
   Краткое руководство ЮНИСЕФ по Конвенции и Факультативным протоколам к ней.

6. **Замечание общего порядка № 25 (2021 г.) о правах детей в отношении цифровой среды**[331]
   Замечание общего порядка № 25 содержит практический анализ того, каким образом права, перечисленные в КПР ООН, применяются к вопросам безопасности детей в Интернете и цифровой среды.

7. **Замечания общего порядка № 25 (2021) КПР ООН о правах детей в связи с цифровой средой (версия для молодежи)**[332]
   Документ описывает права детей в цифровом мире на простом и понятном им языке.

326. Конвенция о правах ребенка, Управление Верховного комиссара Организации Объединенных Наций по правам человека, 1995 г.
327. Конвенция Организации Объединенных Наций о правах ребенка. The Children's Version, Детский фонд Организации Объединенных Наций.
328. Факультативный протокол к Конвенции по правам детей по продаже детей, детской проституции и детской порнографии, Управление Верховного комиссара Организации Объединенных Наций по правам человека, 2002 г.
329. Факультативный протокол к Конвенции о правах ребенка, касающийся участия детей в вооруженных конфликтах, Управление Верховного комиссара Организации Объединенных Наций по правам человека, 2002 г.
330. Факультативный протокол к Конвенции о правах ребенка, касающийся процедуры сообщений, Управление Верховного комиссара Организации Объединенных Наций по правам человека, 2014 г.
331. Как Конвенция ООН о правах ребенка защищает права детей, Детский фонд Организации Объединенных Наций.
332. Своими словами – права детей в цифровом мире, Фонд 5Rights, 2021 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

Другие полезные международные концепции и документы

1. ***Модель национального реагирования*** **(MNR) Глобального альянса WeProtect**[333]
   Модель национального реагирования (MNR) является ключевым элементом любого национального инструментария для обеспечения безопасности детей в Интернете. MNR направлена на оказание помощи странам в разработке мер реагирования на сексуальную эксплуатацию детей и жестокое обращение с ними в Интернете, однако в ней также подчеркивается, что эту проблему невозможно решить изолированно. Для обеспечения комплексных мер национального реагирования необходим более широкий набор возможностей по предотвращению этой проблемы и борьбе с ней. в данном Наборе программных средств представлены ресурсы, способствующие реализации MNR. Набор программных средств для обеспечения безопасности детей в Интернете может помочь сторонам, подписавшим MNR Глобального альянса WeProtect, убедиться в том, что они обладают институциональным потенциалом для реализации его целей и выполнения обязательств, закрепленных в Замечании общего порядка № 25 (2021 г.).

2. **Руководящие принципы Международного союза электросвязи (МСЭ) по безопасности детей в Интернете**[334] Руководящие принципы МСЭ представляют собой всеобъемлющий набор рекомендаций и инструментов для всех соответствующих заинтересованных сторон в отношении того, как создать безопасную интернет-среду, способствующую расширению прав и возможностей детей и молодежи.

   Документ стал результатом совместных усилий 80 экспертов из различных секторов, включая правительства, международные организации, НПО, научные круги и частный сектор. Первоначальная версия, подготовленная в 2009 г., была обновлена в 2020 г. и включила в себя четыре набора руководящих принципов для:

   - ☐ детей;
   - ☐ родителей/опекунов и преподавателей;
   - ☐ представителей отрасли;
   - ☐ законодателей.

3. **Цели ООН в области устойчивого развития (ЦУР)**
   Безопасность детей в Интернете способствует достижению нескольких ЦУР и может стать частью повесток дня законодателей для выполнения их обязательств по ЦУР. Повестка дня в области устойчивого развития на период до 2030 года[335], принятая всеми государствами-членами Организации Объединенных Наций в 2015 г., представляет собой общий план обеспечения мира и процветания для людей и планеты в настоящее время и в будущем. в ее основе 17 Целей устойчивого развития (ЦУР)[336], которые являются настоятельным призывом к действиям для всех стран — как развитых, так и развивающихся — в рамках глобального партнерства. Они признают, что искоренение бедности и других лишений должно идти рука об руку со стратегиями, направленными на улучшение здоровья и системы образования, сокращение неравенства и стимулирование экономического роста — при одновременном решении проблемы изменения климата и работе над сохранением наших океанов и лесов.

4. **Руководящие принципы предпринимательской деятельности в аспекте прав человека, ООН**[337]
   Настоящие руководящие принципы исходят из признания:

   a) принятых государствами обязательств соблюдать, защищать и осуществлять права человека и основные свободы;
   b) роли предприятий, выполняющих специализированные функции в качестве специализированных органов общества, которым предъявляется требование соблюдать все действующие законы и уважать права человека;
   c) необходимости обеспечивать соблюдение прав и обязанностей в случае их нарушения с помощью соответствующих эффективных средств правовой защиты.

   Настоящие руководящие принципы применяются ко всем государствам и ко всем транснациональным и иным предприятиям независимо от их размеров, сферы деятельности, места нахождения, форм собственности и структуры. ▸

333. Модель национального реагирования, Глобальный альянс WeProtect, 2015 г.
334. Руководящие принципы по защите детей в Интернете, Международный союз электросвязи, 2021 г.
335. Преобразование нашего мира: Повестка дня по вопросам устойчивого развития на период до 2030 года, Департамент Организации Объединенных Наций по экономическим и социальным вопросам, 2015 г.
336. 17 целей, Департамент Организации Объединенных Наций по экономическим и социальным вопросам, 2015 г.
337. Руководящие принципы предпринимательской деятельности в аспекте прав человека, Управление Верховного комиссара Организации Объединенных Наций по правам человека, 2011 г.

5. **Программа INSPIRE, инициированная Всемирной организацией здравоохранения: семь стратегий по искоренению насилия в отношении детей**[338]
Разработанный на фактических материалах технический пакет для поддержки действий государств-участников по предотвращению насилия в отношении детей в возрасте от 0 до 17 лет и реагированию на него. Пакет включает в себя базовый документ, в котором описываются стратегии и мероприятия INSPIRE; подробное руководство по их осуществлению; а также набор показателей для оценки степени использования стратегии INSPIRE и ее воздействия на уровни насилия в отношении детей.

6. **Проект Руководства по созданию политики в области искусственного интеллекта для детей, ЮНИСЕФ**[339]
Руководство предназначено для продвижения прав детей в политике и практике искусственного интеллекта в государственном и частном секторе, а также для повышения осведомленности о том, как системы ИИ могут поддерживать реализацию этих прав или препятствовать ей. Документ исследует аспекты и системы искусственного интеллекта, а также описывает их влияние на детей. Он опирается на Конвенцию о правах ребенка, представляя три базовых принципа ИИ, обеспечивающих защиту прав детей:

   - ☐ Политика и системы ИИ должны быть направлены на защиту детей.
   - ☐ Они должны обеспечивать справедливое удовлетворение потребностей и прав детей.
   - ☐ Они должны расширять права и возможности детей с тем, чтобы они могли вносить свой вклад в развитие и использование ИИ.

Опираясь на эти принципы, руководство предлагает девять требований к искусственному интеллекту, ориентированному на ребенка, и предоставляет ресурсы для практической реализации руководства.

7. **Люксембургские руководящие принципы терминологии для защиты детей от сексуальной эксплуатации и сексуальных надругательств**[340]
Эти руководящие принципы представляют собой инициативу 18 международных партнеров по согласованию терминов и определений, касающихся защиты детей. Они направлены на повышение концептуальной ясности терминологии с тем, чтобы обеспечить более решительную и последовательную просветительскую деятельность, политику и законы на всех языках во всех регионах мира.

8. **Принцип предотвращения**[341]
ЮНЕСКО совместно со своим консультативным органом Всемирной комиссией по этике научных знаний и технологий разработала рабочее определение «принципа предотвращения», которое содержится во многих международных документах, касающихся научных разработок в целом, и в том числе ориентированных на детей:

   «Когда деятельность человека приводит к морально неприемлемому ущербу, который является научно обоснованным, но неопределенным, необходимо принять меры для предотвращения или снижения такого ущерба. Под морально неприемлемым ущербом понимается вред, причиненный человеку или окружающей среде, который:

   1. представляет угрозу жизни или здоровью человека;
   2. является серьезным и практически необратимым;
   3. является несправедливым по отношению к нынешнему или будущим поколениям;
   4. наносится без надлежащего учета прав пострадавших. ▸

338. Программа INSPIRE: семь стратегий по искоренению насилия в отношении детей, Всемирная организация здравоохранения, 2021 г.
339. Руководство по созданию политики в области искусственного интеллекта для детей, Детский фонд Организации Объединенных Наций, 2020 г.
340. Универсальная терминология: Терминологическое руководство по защите детей от сексуальной эксплуатации и сексуального насилия, ECPAT International, 2016 г.
341. Принцип предотвращения, Всемирная комиссия по этике научных знаний и технологий, 2005 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

Оценка обоснованности должна полагаться на научный анализ. Чтобы выбранные действия подлежали постоянному пересмотру, характер такого анализа должен быть непрерывным. Неопределенность может относиться к причинным связям или границам возможного ущерба, но не обязательно ограничиваться ими.

Действия — это меры, предпринимаемые до причинения вреда и направленные на его предотвращение или снижение. Следует выбирать действия, соразмерные серьезности потенциального вреда, с учетом их позитивных и негативных последствий, а также оценкой моральных последствий как действий, так и их отсутствия. Выбор действий должен быть результатом процесса, основанного на широком участии общественности».

9. **Региональные нормативные документы по вопросам защиты прав детей**
   Например, Руководящие принципы[342] Совета Европы по уважению, защите и осуществлению прав ребенка в цифровой среде являются полезным руководством в европейском контексте. Африканский союз разработал Африканскую хартию прав и основ благополучия ребенка[343] для описания прав детей в африканском контексте.

10. **Инновационные национальные разработки, имеющие глобальное значение**
    Например, британский Закон о проектах, учитывающих возрастные ограничения[344] и австралийский Закон о безопасности в Интернете.[345]

342. Руководящие принципы по уважению, защите и соблюдению прав ребенка в цифровой среде, Совет Европы, 2018 г.
343. Африканская хартия прав и основ благополучия ребенка, Африканский союз, 1990 г.
344. Введение в закон о проектах, учитывающих возрастные ограничения, Управление уполномоченного по вопросам информации.
345. Консультации по новому Закону о безопасности в Интернете, Департамент инфраструктуры, транспорта, регионального развития и связи.

СИСТЕМНАЯ ПАПКА

8 ДОКУМЕНТОВ | 105 МБ НА ДИСКЕ | РАЗДЕЛ 7

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

Глоссарий

В рамках своей восемьдесят шестой сессии Комитет по правам ребенка принял Замечание общего порядка № 25 (2021 г.) о правах детей в отношении цифровой среды. Данный терминологический глоссарий также включен в упомянутый документ, однако не является исчерпывающим.

Вспомогательные технологии
Технологии, разработанные для поддержки или повышения независимости человека, включая адаптивные и реабилитационные системы и устройства для людей с ограниченными возможностями, такие как программа для чтения экрана или распознавание речи.

Автоматизированная обработка
Процесс принятия решений с помощью автоматизированных средств, т. е. с использованием программного обеспечения, настроенного для анализа предоставленных данных и соблюдения установленных правил для принятия решений на основе алгоритмов без участия человека.

Автоматизированный поиск
Процесс оценки данных для фильтрации контента, к которому пользователи получают доступ в Интернете. в основном используется в коммерческих целях. Подбор контента осуществляется на основе анализа реакции пользователя на другие материалы или на основе материалов, которые ищут другие пользователи, действующие аналогичным образом.

Автоматизированные системы
Программное и аппаратное обеспечение, запрограммированное на автоматическое выполнение функции без необходимости вмешательства человека для предоставления входных данных и инструкций для каждой операции.

Поведенческое целеполагание
Анализ действий пользователей в Интернете с целью таргетирования рекламы, сообщений, рекомендаций по контенту или контактов с другими пользователями на основе их предыдущих предпочтений, часто с целью манипулирования их будущим поведением.

Риски, связанные с контентом
Потенциальный вред для пользователей, связанный с характером интернет-контента, в том числе такими его категориями, как не соответствующий возрасту (например, порнография), ненадежный (например, ложные сведения или дезинформация) или какой-либо другой (например, побуждающий к рискованному поведению либо описывающий способы нанесения себе вреда или самоубийства).

Риски контакта
Потенциальный вред, возникающий из-за возможности пользователей контактировать друг с другом с помощью онлайн-сервисов, которые, например, позволяют незнакомцам или людям, скрывающим свою личность, связываться с детьми.

Поведенческие риски
Потенциальный вред, основанный на поведении пользователя или связанных с ним лиц, например, преднамеренное использование онлайн-платформ для угроз или преследования других пользователей, включая кибербуллинг, «секстинг» и ненавистнические комментарии, иногда также непреднамеренные — путем раскрытия частной информации других пользователей.

Риски, связанные с договоренностями
Потенциальный вред, связанный с неприемлемыми коммерческими договорными отношениями или давлением, например принудительное использование, азартные игры, таргетированная реклама, скрытые расходы, несправедливые условия использования, а также потеря контроля над персональными данными.

< ПРЕДЫДУЩИЙ РАЗДЕЛ СЛЕДУЮЩИЙ РАЗДЕЛ >

Модерация контента
Практика мониторинга и проверки пользовательского контента по заранее определенным правилам в отношении удаления недопустимого содержимого автоматическим способом либо с помощью модераторов. Модерация контента может выполняться одновременно с его созданием, как в чатах, или с задержкой, как на форумах.

Киберагрессия
Действия, совершаемые отдельными лицами или группами лиц в Интернете либо с использованием цифровых технологий, часто с намерением нанести оскорбление вред или ущерб другому лицу или группе лиц.

Минимизация объема информации
Принцип сбора минимального количества персональных данных, необходимых исключительно для цели, в которой они обрабатываются, и их хранения только в той мере, в какой это необходимо для достижения цели.

Обработка данных
Включает процессы сбора, регистрации, хранения, анализа, распространения и использования данных.

Компьютерная грамотность
Способность использовать информационно-коммуникационные технологии для поиска, оценки, создания и коммуникации. Смежными терминами, в частности, являются «медийная грамотность», «информационная грамотность» или «медийная и информационная грамотность».

Преобразование в цифровую форму
Адаптация среды, деятельности, бизнеса и повседневной жизни для включения в них цифровых услуг и инфраструктуры, а также использования их преимуществ. Это также относится к преобразованию информации в цифровой формат.

Дезинформация
Распространение заведомо ложной информации.

Эмоциональная аналитика
Сбор данных для определения настроения человека и влияния на него, часто проводимый путем оценки видео, голоса, письменных коммуникаций или персональных данных в целях идентификации таких характеристик, как выражение лица и тон, коррелирующих с конкретными эмоциями, с использованием методов машинного обучения, включая алгоритмы.

Хищение персональных данных
Мошенническая выдача себя за другое лицо, например с целью доступа к его имуществу или контактам в Интернете, нанесения вреда репутации или получения выгоды другими способами.

Иммерсивная реклама
Незаметная интеграция рекламы в интернет-контент или цифровые услуги, позволяющая пользователям оставаться погруженными в контент и функции сервисов, одновременно подвергаясь влиянию бренд-маркетинга и сообщений.

Технология внедрения
Микрочип, который может быть имплантирован в человека для хранения, отслеживания или извлечения информации, содержащейся во внешней базе данных, такой как личная идентификация и/или медицинские, правоохранительные или контактные сведения.

Фильтрование информации
Использование программы для проверки цифрового контента с целью поиска или скрытия информации, соответствующей установленным критериям. Распространенными способами фильтрования информации являются скрытие оскорбительного контента в результатах поиска или сортировка, в которой нужные результаты отображаются первыми.

Ложные сведения
Распространение ложной информации без умышленного вреда.

Нейромаркетинг
Изучение того, как человеческий мозг реагирует на маркетинговый контент, и применение этих знаний для разработки более эффективных маркетинговых кампаний. Реакции могут быть измеряться широким спектром способов: от сканирования активности мозга до продолжительности взаимодействия, переходов и времени, проведенного на сайте.

Встроенный алгоритм конфиденциальности
Практика разработки онлайн-сервисов с целью максимально возможной защиты конфиденциальности пользователей, например путем автоматической настройки аккаунтов несовершеннолетних лиц как частных или путем сведения к минимуму объема собираемых данных.

Составление профиля
Практика использования персональных данных для определения, прогнозирования или анализа характеристик пользователя, включая его реакции (нравится/не нравится), предпочтения, взгляды, мнения или поведение, для рекомендации контента, продуктов или услуг на основе профиля данных человека.

Встроенная безопасность
Практика разработки онлайн-сервисов с целью обеспечения максимально возможной безопасности пользователей, например автоматические настройки безопасности для аккаунтов несовершеннолетних или предотвращение их контактов со взрослыми.

Таргетированная реклама
Практика показа определенной рекламы пользователям на основе собранных о них данных, например об их онлайн-активности, покупках, местоположении, гендере, возрасте, предпочтениях и т. д.

Виртуальная и дополненная реальность

Виртуальная реальность —
компьютерное моделирование трехмерного изображения или среды, с которой человек может взаимодействовать с виду реальным или физическим образом, с использованием специального цифрового оборудования, такого как шлем с экраном внутри или перчатки с датчиками.

Дополненная реальность —
моделирование физического мира с измененными характеристиками или дополненными элементами, обычно передаваемое через экран, чтобы обеспечить наложение виртуальных объектов на живое изображение или видео.

Дополнительные термины, касающиеся сексуального насилия над детьми, см. в Люксембургских руководящих принципах ECPAT.[346]

346. Универсальная терминология: Терминологическое руководство по защите детей от сексуальной эксплуатации и сексуального насилия, ECPAT International, 2016 г.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

Послесловие

Обеспечение защиты детей в Интернете является делом рук многих: мировых лидеров, международного сообщества, законодателей, правоохранительных органов, специалистов в области здравоохранения, учителей, родителей, опекунов и самих детей.

< ПРЕДЫДУЩИЙ РАЗДЕЛ

СЛЕДУЮЩИЙ РАЗДЕЛ >

СИСТЕМНАЯ ПАПКА

8 ДОКУМЕНТОВ	105 МБ НА ДИСКЕ	РАЗДЕЛ 8

Проект типовой политики

Приведенный ниже текст представляет собой проект типовой политики, объединяющей все разделы настоящего Набора программных средств. У каждой страны своя отправная точка для разработки политики безопасности детей в Интернете. Данная модель позволяет решать вопросы, связанные с цифровыми аспектами прав детей.

Введение

Важность соблюдения прав детей

Права детей являются неотъемлемой частью любой политики, затрагивающей жизнь детей как в Интернете, так и за его пределами. Цель политики обеспечения безопасности детей в Интернете, по сути, заключается в том, чтобы право детей на защиту и участие было реальным и эффективным в процессе их взаимодействия с цифровым миром.

Права детей и их семей закреплены в Международном билле о правах, включая Всеобщую декларацию прав человека 1948 года, Международный пакт о гражданских и политических правах 1966 года и Международный пакт об экономических, социальных и культурных правах 1966 года, а также в региональных и национальных структурах по правам человека.

В том, что касается конкретно детей, Конвенция Организации Объединенных Наций о правах ребенка 1989 года («Конвенция» или КПР)[1] вместе с Факультативными протоколами к ней, касающимися вопросов торговли детьми[2] и участия детей в вооруженных конфликтах[3], обеспечивают практическую основу для понимания того, как права человека применяются к детям. Конвенция — это договор по правам человека, который ратифицировали наибольшее количество государств в истории, а Факультативный протокол к ней, касающийся процедуры сообщений, помогает обеспечить ее исполнение с тем, чтобы права детей имели реальное применение и юридическую силу.

Все права, содержащиеся в КПР, направлены на безопасность детей в Интернете, в то время как консультации с детьми имеют решающее значение для понимания того, что эти права означают на практике. Например, следует рассмотреть вопрос о правах детей на игру, участие и семейную жизнь в онлайн-пространстве. Все, кто участвует в проведении консультаций, должны пройти надлежащую подготовку по вопросам прав детей, учета мнений детей и их вовлечения в жизнь общества.

5 основных соображений

1. Как выявлять риски и смягчать их последствия

Стратегии обеспечения безопасности детей в Интернете должны разрабатываться в первую очередь так, чтобы дети получали максимальную выгоду от использования цифровых технологий. Это подразумевает первостепенную ответственность за снижение рисков, минимизацию вероятности причинения вреда, устранение вреда в случае его причинения, а также анализ того, как продукция и услуги могут повлиять на конечного пользователя, если этим пользователем является (или может являться) ребенок. Ключевое значение имеет разработка продуктов и услуг, которые предполагают безопасное участие детей.

В то время как некоторым детям причиняется серьезный вред, миллионы других детей в Интернете подвержены ему в той или иной форме. Например, существует широкий спектр рисков, связанных с коммерческим наблюдением или эксплуатацией, распространением ложной информации или мошенничеством, преследованием или буллингом. Меньшее число детей страдает от серьезного вреда, причиняемого сексуальным насилием. Многие риски являются совокупными. Они сказываются на разных детях по-разному, и одна форма вреда может открывать возможности для других его форм.[4]

Глобальный характер цифрового мира означает, что дети сталкиваются с одинаковыми рисками независимо от своего географического положения. Однако в различных контекстах могут возникать специфические проблемы. в некоторых случаях дети могут оказаться в невыгодном положении из-за отсутствия доступа к Интернету. в других случаях может существовать связь между вредом, нанесенным в сети, и опытом ребенка в реальной жизни. Конкретные риски и вред часто накладываются друг на друга. Существует очень мало прямых взаимосвязей или точных классификаций.

---

1. Конвенция о правах ребенка, Управление Верховного комиссара Организации Объединенных Наций по правам человека, 1989 г.
2. Конвенция о правах ребенка, Управление Верховного комиссара Организации Объединенных Наций по правам человека, 1989 г.
3. Конвенция о правах ребенка, Управление Верховного комиссара Организации Объединенных Наций по правам человека, 1989 г.
4. Построение цифрового мира, которого заслуживает молодежь, Фонд 5Rights, 2020 г.

Такие факторы, как гендер, возраст, семейные обстоятельства, социально-экономический статус, местоположение, опыт и доступность цифровых технологий, могут менять характер рисков и способы причинения вреда детям. Некоторые риски и вред затрагивают целые сообщества и группы детей: например, девочки чаще испытывают на себе жестокое обращение, а мальчики сталкиваются с более серьезными его проявлениями.[5] Культурные нормы, связанные с мужественностью, также усугубляют проблему выявления случаев сексуального надругательства над детьми мужского пола и недостаточного сообщения о них.[6] Риски и вред могут также усиливаться платформами, которые по замыслу поощряют обмен шокирующим и сенсационным контентом: они могут профилировать или продвигать определенные типы поведения пользователей, поскольку это стимулирует выгодное взаимодействие.

Законодатели должны учитывать все риски для детей и принимать меры по их смягчению. Ключевым инструментом для выявления рисков является концепция 4C.

Классификация 4 рисков, разработанная проектом CO:RE (CO:RE 4Cs), признает, что онлайн-риски возникают, когда ребенок:

- взаимодействует с потенциально вредным **контентом** и/или подвергается его воздействию;
- устанавливает **контакт** с потенциально опасным человеком и/или становится его целью;
- становится свидетелем, участником и/или жертвой потенциально вредного **поведения**;
- является стороной потенциально опасного **договора** и/или эксплуатируется в соответствии с ним.

2. Как обеспечить доступ к информационным технологиям, доступность информации и взаимодействие всех заинтересованных сторон

Сегодня доступ к Интернету имеет решающее значение для осуществления детьми своих прав и полного раскрытия их потенциала. Политика безопасности ребенка в Интернете должна быть инклюзивной как по замыслу, так и на практике.[7] Это означает, что она должна опираться на достаточное количество информации, а также существующую передовую практику и нормативные рамки, особенно в ситуациях ограниченных ресурсов. Вне зависимости от того, означает ли реализация политики безопасности детей в Интернете адаптацию существующего законодательства (например, в отношении защиты детей, защиты потребителей или регулирования телекоммуникаций) к конкретным условиям или создание новых сводов законов, она должна способствовать интеграции и равенству для всех детей, независимо от того, кто они и где находятся.

Дети не являются однородной группой. Политика безопасности детей в Интернете должна быть доступной и инклюзивной, чтобы охватить всех детей, независимо от того, кто они и где проживают. «Цифровой разрыв» может возникнуть в тех случаях, когда некоторые дети могут легко получить доступ к цифровому пространству, а у других такой возможности фактически нет. Нормативные рамки должны соответствовать возрасту и работать для всех детей независимо от пола, расы, религии, национальности, этнической принадлежности, инвалидности или любых других характеристик. Формулировки должен быть понятными и инклюзивным, а материалы, при необходимости, — доступны на различных языках. Материалы по безопасности детей в Интернете должны разрабатываться на основе консультаций с детьми и родителями/опекунами: как минимум, они должны соответствовать возрасту, быть нейтральными с гендерной точки зрения и легкодоступными для детей разных возрастов и их родителей/опекунов. в случае ограничений, связанных с грамотностью, более эффективными часто являются визуальные материалы. Единообразие терминологии на различных платформах обеспечивает большую доступность информации о безопасности детей в Интернете для детей, их семей и опекунов.[8]

Законодатели должны содействовать доступу детей к Интернету и вовлекать их в процесс создания безопасной цифровой среды.

---

5. Результаты инвестиционного портфеля инициативы «Безопасность в Интернете» (Safe Online) за 2020 год, Глобальное партнерство по борьбе с насилием в отношении детей, 2020 г., стр. 2.
6. Предотвращение нарушений в Кении: данные о сексуальной эксплуатации детей в Интернете и жестоком обращении с ними, Глобальное партнерство по борьбе с насилием в отношении детей, 2021 г., стр. 68.
7. Например: дети с ограниченными возможностями или дети из маргинализированных групп меньшинств, беспризорные дети, перемещенные дети и дети мигрантов, среди прочих. Данная проблема более подробно обсуждается ниже в рамках межсекторальных вопросов. Более подробную информацию о модели и контрольном списке можно найти в публикации «Одного "голоса" недостаточно: концептуализация статьи 12 Конвенции ООН о правах ребенка», Лора Ланди, 2013 г.
8. См. введение о важности формулировок и определений и раздел «Глоссарий».

3. Как построить цепочку ответственности

Ответственность за обеспечение безопасности детей в Интернете лежит на многих людях, специалистах и организациях, включая правительство, правоохранительные органы, бизнес, педагогов, службы психологической и социальной поддержки, семьи и самих детей. Некоторые звенья в этой цепочке несут большую ответственность, чем другие.[9] Например, разработчики сервиса, доступ к которому может быть предоставлен детям или который может повлиять на них, должны учитывать, представляет ли какая-либо из функций риск для детей. Это необходимо сделать до того, как привлекать детей к использованию такого сервиса. Это часто называют «встроенной безопасностью» или «проектами, учитывающими интересы детей». Встроенная безопасность должна быть нормой.

Ответственность за безопасность детей в Интернете включает в себя как предотвращение вреда, так и принятие мер по его смягчению и устранению. Инструменты подачи жалоб и сообщений о нарушениях должны быть доступными и четко обозначенными, чтобы дети, опекуны и специалисты, которые в них нуждаются, могли легко находить и использовать их. в рамках цифровых коммерческих систем следует создать механизмы, позволяющие отслеживать и оценивать сообщения о нарушениях. Это позволит оперативно выявлять и решать проблемы.

Законы и нормативные акты должны устанавливать четкие рамки для предотвращения проблем, а также несения ответственности и возмещения вреда в случае их возникновения. Это включает сбор данных о сообщениях и жалобах, чтобы они контролировались и анализировались в целях совершенствования системы. Дети и родители/опекуны не должны нести ответственности за предотвращение или устранение рисков и вреда, которые они плохо понимают или не могут контролировать. Согласие не может использоваться для освобождения государственных или частных организаций от их ответственности за безопасность детей в Интернете. Включение вопросов безопасности детей в Интернете в существующие механизмы обеспечения[10] безопасности продуктов[11], защиты детей, прав детей[12] и прав потребителей[13] поможет устранить пробелы в цепочке ответственности и дублирования ресурсов, ролей и обязанностей. Не должно существовать никаких правовых лазеек, снижающих эффективность защиты детей в Интернете.

Крайне важно, чтобы безопасность детей в Интернете была интегрирована во все соответствующие области политики, начиная с национальных планов развития широкополосной связи и заканчивая учебными программами. Интеграция должна быть выполнена таким образом, чтобы она была прозрачной, подотчетной и реализуемой. Создание разрозненных систем может привести к возникновению конфликтов в области регулирования и фрагментации процесса разработки и осуществления политики.

4. Как добиться того, чтобы проект учитывал интересы детей

Безопасность детей в Интернете должна учитываться при проектировании и разработке технологий. в сервисах и продуктах, учитывающих интересы ребенка, его безопасность в Интернете является встроенной по умолчанию. в частности, речь идет о ее включении в нормативные требования к проектированию и лицензированию новых технологий[14]. Проекты, учитывающие интересы детей, также можно назвать проектами со встроенными безопасностью, правами, конфиденциальностью и этикой.

Применение принципа предотвращения[15] к технологиям, которые могут повлиять на детей и молодежь, гарантирует учет принципа безопасности детей в Интернете на самой ранней стадии разработки. Всемирная комиссия ЮНЕСКО по этике научных знаний и технологий (КОМЕСТ) предложила «рабочее определение» принципа предотвращения:

«Когда деятельность человека приводит к морально неприемлемому ущербу, который является научно обоснованным, но неопределенным, необходимо принять меры для предотвращения или снижения такого ущерба.

---

9. См., например, Руководящие принципы предпринимательской деятельности в аспекте прав человека, ООН.
10. Центр защиты детей, Европейская комиссия, 2021 г.
11. Стратегия по правам ребенка, Совет Европы, 2021 г.
12. Директива по правам потребителей, Европейская комиссия, 2014 г.
13. Руководящие указания для директивных органов по защите ребенка в онлайновой среде, Международный союз электросвязи, 2020 г.
14. Добровольные принципы противодействия сексуальной эксплуатации детей и жестокому обращению с ними в Интернете, GOV.UK, 2021 г.
15. См. Сообщение Комиссии о принципе предотвращения, EUR-Lex, 2000 г.; Принцип предотвращения: определения, применение и управление, Европейский парламент, 2015 г.

Под морально неприемлемым ущербом понимается вред, причиненный человеку или окружающей среде, который:

- представляет угрозу жизни или здоровью человека;
- является серьезным и практически необратимым;
- является несправедливым по отношению к нынешнему или будущим поколениям;
- наносится без надлежащего учета прав пострадавших».[16]

Принцип предотвращения должен лежать в основе концепции встроенных безопасности и конфиденциальности для обеспечения безопасности детей в Интернете и включения их прав в технологию на этапе проектирования. Учет интересов детей должен быть не только этической концепцией, но и юридическим требованием.[17] Он также должен стать одним из критериев финансирования научно-исследовательской работы, которая может затрагивать права детей в Интернете.

Технологии и искусственный интеллект (ИИ) способны повысить безопасность детей в Интернете и защитить их права. Одним из важных аспектов политики в этой области является содействие разработке технических средств для реализации прав детей и повышения их безопасности в Интернете. Более широкое воздействие ИИ или других технологий, предназначенных для защиты детей, должно оцениваться в свете всех прав ребенка,[18] чтобы не подрывать некоторые из них: например, право на неприкосновенность частной жизни и недискриминацию.

Дети являются чрезвычайно неоднородной группой, и при разработке, осуществлении и мониторинге эффективности политики в этой области следует учитывать весь спектр характеристик и условий жизни детей. Эффективные действия по обеспечению безопасности детей в Интернете должны быть направлены на устранение существующих противоречий. Например, в дебатах по шифрованию аргументы сторонников борьбы с сексуальной эксплуатацией детей и жестоким обращением с ними (CSEA) могут противоречить аргументам, связанным с конфиденциальностью и защитой данных. Такие конфликты должны разрешаться в той мере, в какой это возможно на практике с тем, чтобы избежать многолетних дискуссий, в то время как дети подвергаются риску или страдают. в таких случаях интересы ребенка должны иметь первостепенное значение.[19]

Существует несколько механизмов и процессов, которые поддерживают проекты, учитывающие интересы ребенка, при разработке политики, включая принцип предотвращения, оценку воздействия на права детей[20] и их консультирование.[21]

Кроме того, Ассоциация стандартов Института инженеров электротехники и электроники (IEEE-SA) разработала стандарт, предусматривающий практические шаги, которым компании могут следовать для разработки цифровых продуктов и услуг с учетом возраста пользователей,[22] а Комиссия по цифровым перспективам определила, как право детей на свободную игру может быть поддержано в цифровом мире путем улучшения дизайна продуктов и услуг. Законодатели должны всегда стремиться к тому, чтобы разработчики сводили к минимуму риск, прежде чем их продукты и услуги станут доступными для детей.

Принципы встроенных безопасности и прав носят системный характер и поэтому направлены на защиту миллионов детей с самого начала, а не после того, как что-то случится.

5. Как обеспечить эффективность системы

Безопасность детей в Интернете и защита их прав в цифровой среде могут быть по-настоящему эффективными только при наличии практических политических действий, достаточного финансирования и правоохранительных мероприятий.

Безопасность детей в Интернете имеет отношение к широкому кругу областей политики, включая информационно-коммуникационные технологии (ИКТ), образование, уголовное правосудие, здравоохранение, регулирование отрасли, социальную и семейную поддержку, предпринимательство, права человека и равенство, международное развитие и многие другие.

---

16. Принцип предотвращения, Всемирная комиссия по этике научных знаний и технологий, 2005 г.
17. См. например, статью 25 Общего регламента о защите данных, Европейский союз, 2018 г.
18. См. например, Замечание общего порядка № 25 (2021 год) о правах детей в отношении цифровой среды, Конвенция Организации Объединенных Наций о правах ребенка (UNCRC), 2021 г.
19. Конвенция о правах ребенка, Управление Верховного комиссара Организации Объединенных Наций по правам человека, 1989 г. (См., в частности, раздел 1 статьи 3 о правах детей).
20. Оценка воздействия на права ребенка, Комиссия по цифровым перспективам, 2021 г.
21. Оценка воздействия на права ребенка, Комиссия по цифровым перспективам, 2021 г.
22. Стандарт для рамочных цифровых услуг с учетом возраста IEEE 2089-21, IEEE SA, 2021 г.

Таким образом, сотрудничество между различными министерствами и ведомствами, работающими в стратегических областях, имеет важнейшее значение для эффективной деятельности по обеспечению безопасности детей в Интернете. Чтобы обеспечить ресурсы для осуществления политики как в рамках различных департаментов, так и между ними, необходимо финансирование. Политика с недостаточным финансированием или партнерство без возможностей, то есть то, что существует только на бумаге, не приведет к эффективной защите детей в Интернете.

Понимание принципов эффективности означает пересмотр влияния политики на безопасность детей в Интернете. Мониторинг, оценка и сбор данных являются ключевыми факторами для разработки качественной политики. Одним из лучших способов максимального повышения эффективности является извлечение уроков и обмен опытом в области разработки эффективной трансграничной политики. Проверка эффективности политики обеспечения безопасности детей в Интернете требует проведения консультаций не только с основными заинтересованными сторонами, но и с детьми. Это позволит понять, каким образом предусмотренные в политике меры влияют или могут повлиять на них в будущем.[23] Это непрерывный процесс.

Политика должна быть основана на данных и фактах. Как соответствующие органы, так и частные компании должны собирать данные и обмениваться ими в целях лучшего понимания проблем в области безопасности детей в Интернете в соответствии с законами и принципами защиты данных. Безопасность детей в Интернете является относительно новой областью политики, поэтому в тех случаях, когда доказательства отсутствуют или оспариваются, законодатели должны применять принцип предотвращения или использовать эффективные подходы, работающие в других условиях: например, обращаться к областям здравоохранения или безопасности либо к таким концепциям, как «Семь стратегий по искоренению насилия в отношении детей» (INSPIRE).[24]

Безопасность детей в Интернете не является обособленной проблемой. Эффективность политики в этой области будет зависеть от общей продуктивности ключевых учреждений и их способности сотрудничать в целях обеспечения надежной защиты. Обеспечение эффективной подотчетности в области безопасности детей в Интернете в целом и предотвращение сексуальной эксплуатации детей и жестокого обращения с ними (CSEA) в частности основывается на сильной национальной системе правосудия. Руководство по этому вопросу содержится в Модели национального реагирования (MNR).

Эффективные подходы к обеспечению безопасности детей в Интернете также зависят от наличия достаточных ресурсов для соответствующих учреждений, в том числе в таких областях, как психологическая и социальная поддержка, а также регулирование ИКТ и смежных сфер. Эффективная защита прав ребенка с помощью политики обеспечения безопасности детей в Интернете зависит от действенного законодательства в области прав человека, а также конкретных законов и регулирования со стороны органов надзора в целях, гарантирующих права детей как в цифровой среде, так и в реальной жизни.

Законодатели должны обеспечить наличие возможностей вовлеченных организаций, ресурсов и механизмов подотчетности для поддержки политики обеспечения безопасности детей в Интернете. в случае возникновения конфликтов первостепенное значение должны иметь интересы ребенка. Без этого даже самая качественная политика будет неэффективной.

Области применения политики

1. Возможности вовлеченных организаций

1a. Подтвердить государственную поддержку вопросам безопасности детей в Интернете на самом высоком уровне
Национальные лидеры, включая премьер-министра или президента, должны взять на себя обязательство обеспечивать безопасность детей в Интернете как на национальном, так и на международном уровнях.

1b. Назначить министерство или ведомство, которое возьмет на себя ведущую роль при разработке национальной политики безопасности детей в Интернете
Во всем мире целый ряд различных учреждений и министерств играют ведущую роль в разработке политики безопасности детей в Интернете. Выбор такого учреждения или министерства может повлиять на то, как будет развиваться политика и каким аспектам будет уделено наибольшее внимание. Безопасность детей в Интернете, вероятно, будет вопросом, рассматриваемым в нескольких министерствах, однако за повестку дня должно отвечать одно ведущее ведомство. в некоторых странах такая политика осуществляется под руководством министерства по вопросам ИКТ, в других — министерства по делам детей и семей или юстиции. Существующие группы, отвечающие за вопросы насилия в отношении детей (VAC) или кибербезопасности, могут быть расширены с тем, чтобы включить в них необходимый экспертный потенциал для предотвращения изолированной работы. Ведущее ведомство может быть

23. Комиссия по цифровым перспективам, Фонд 5Rights, 2021 г.
24. Руководство по показателям и матрица результатов программы INSPIRE, Всемирная организация здравоохранения, 2018 г.

выбрано с учетом его авторитета, опыта, ресурсов, потенциала или энтузиазма, однако важным условием является его сотрудничество с другими учреждениями. Независимо от того, какое министерство возьмет на себя ведущую роль, оно должно придерживаться целостного подхода, отражающего все потребности, связанные с безопасностью детей в Интернете.

1c. Опубликовать руководство по терминологии и языку
Назначенное ведущее министерство должно опубликовать полный перечень терминов и формулировок, используемых в международной передовой практике.[25]

1d. Создать Национальный руководящий комитет по безопасности детей в Интернете
Национальный руководящий комитет по безопасности детей в Интернете должен отвечать за осуществление и разработку политики, а также выполнять функции координационного центра по вопросам национального и регионального сотрудничества. в его задачи будет входить использование Набора программных средств для обеспечения безопасности детей в Интернете и разработка плана действий по его реализации. Комитет будет заниматься широким кругом вопросов, охватывающих различные области политики, включая, в частности, образование, здравоохранение, правосудие, защиту потребителей, защиту данных, правоохранительную деятельность, информационно-коммуникационные технологии, а также услуги для семьи и детей, и контролировать внедрение и поддержку стандартов. Комитет должен официально сотрудничать со всеми учреждениями, ответственными за безопасность или кибербезопасность детей, и регулярно отчитываться перед ведущим министерством.

1e. Выявить заинтересованные стороны в области безопасности детей в Интернете.
Сотрудники правоохранительных органов, бизнес, третий сектор, организации по защите прав детей, образовательные учреждения, родители/опекуны и научные круги могут стать источником важной информации в области безопасности детей в Интернете. в некоторых условиях создание группы заинтересованных сторон может быть полезным для поддержки Комитета в его деятельности и обоснования плана действий в реальных сценариях. в других контекстах более эффективными могут быть неформальные дискуссии или получение необходимой информации из открытой сети заинтересованных сторон. в любом случае Национальный руководящий комитет по безопасности детей в Интернете должен стремиться к взаимодействию с ключевыми заинтересованными сторонами, которые могут поддержать его деятельность. Следует поощрять межведомственное сотрудничество. Целью вовлечения заинтересованных сторон является сосредоточение внимания на осуществлении, а не на разработке политики.

1f. Определить роли и обязанности заинтересованных сторон
Должна существовать совместная нормативно-правовая база, определяющая роли и обязанности всех организаций, разрабатывающих цифровую инфраструктуру, сети и сервисы, а также управляющих ими, и обязанности государственных ведомств. Следует установить минимальные стандарты для всех участников цепочки создания стоимости, включая тех, кто отвечает за инфраструктуру, аппаратные средства и цифровые продукты и услуги, а также тех, кто управляет ими или использует их при взаимодействии с детьми. Эти стандарты должны быть сосредоточены на безопасности детей и полной реализации их прав в цифровом мире. Следует обеспечить участие гражданского общества и консультирование детей в группах заинтересованных сторон.

1g. Определить показатели эффективности и систему оценки
Для каждого аспекта плана реализации необходимо назначить ответственного (лицо, учреждение, орган) и обеспечить человеческие и финансовые ресурсы для успешного выполнения поставленной задачи. Один орган
может отвечать сразу за несколько областей политики или только за одну из них. Чтобы Руководящий комитет мог осуществлять надзор и отслеживать прогресс, следует внедрить ключевые показатели эффективности (KPI), механизмы оценки и четкие структуры отчетности. в связи с быстрым развитием цифровой среды KPI необходимо постоянно пересматривать.

1h. Обеспечить интеграцию вопросов безопасности детей в Интернете во все области государственной политики
Любые соответствующие национальные планы, такие как Национальный план широкополосной связи или концепция компьютерной грамотности, должны включать политику безопасности ребенка в Интернете в качестве части стратегии реализации. Планы, которые осуществляются в течение нескольких лет, должны пересматриваться на ключевых этапах.

25. См., например, Универсальная терминология: Терминологическое руководство по защите детей от сексуальной эксплуатации и сексуального насилия, ECPAT International, 2016 г.

2. Нормативно-правовое регулирование

2a. Ужесточать законы, запрещающие правонарушения в области безопасности детей в Интернете, и обеспечивать соблюдение таких законов
Уголовное законодательство и процедуры способствуют расследованию и судебному преследованию киберпреступлений, нарушающих право детей на защиту, и должны быть усилены и изменены в соответствии с международными стандартами и передовой практикой. Речь идет о введении обязательной оценки рисков для снижения потенциального вреда, а также, при необходимости, усилении ответственности и наказании. Также необходимо включить процедуры уведомления о нежелательном контенте и его удаления. Уголовное законодательство, касающееся безопасности детей в Интернете, должно разрабатываться с учетом всех прав ребенка, включая право быть выслушанным и право на участие.[26]

2b. Установить правила защиты данных и создать независимые органы надзора, обеспечивающие надлежащую защиту данных детей и их сбор только в случае необходимости и с высоким уровнем безопасности
Такие общие правила должны предусматривать особую категорию для детских данных, автоматически требующую более высокого уровня защиты и гарантий, а также защиту от ненадлежащего коммерческого использования данных о детях. в тех случаях, когда у детей или родителей/опекунов запрашивается согласие на сбор и обработку данных о несовершеннолетних, такое согласие должно быть информированным и осознанным. в исключительных обстоятельствах, когда это отвечает наилучшим интересам ребенка, особое внимание следует уделять сбору данных в целях обеспечения безопасности.

2c. Усилить уголовное расследование, преследование и наказание за сексуальную эксплуатацию детей или жестокое обращение с ними в Интернете[27]
Сотрудники уголовной юстиции, занимающиеся правонарушениями, связанными с безопасностью детей в Интернете, должны пройти обучение в этой области в целях содействия более активному предупреждению, успешному судебному преследованию, вынесению надлежащего наказания, а также более глубокому пониманию последствий для жертв. Следует пересмотреть и укрепить потенциал следственных групп и оперативников в целях выявления, предотвращения и реагирования на угрозы кибербезопасности, особенно когда они связаны с безопасностью детей в Интернете. Системы уголовной юстиции должны быть в состоянии обеспечить своевременный доступ к правосудию.

2d. Оценить и укрепить системы ювенальной юстиции
Обеспечить ясность и соразмерность законодательства для сведения к минимуму риска нарушения закона со стороны ребенка в контексте безопасности детей в Интернете. в тех случаях, когда ребенок сталкивается с уголовным наказанием, связанным с безопасностью детей в Интернете, например, в связи с кибербуллингом или сексуальными надругательствами на основе изображений, система правосудия должна прилагать все усилия для предотвращения криминализации детей и обеспечивать надлежащую поддержку и юридическое представительство нарушителей для защиты их прав.

2e. Выявить и ратифицировать международные договоры и протоколы, касающиеся безопасности детей в Интернете
Создание устойчивой экосистемы безопасности детей в Интернете требует многостороннего подхода и глобального участия. Каждая страна должна определить и ратифицировать соответствующие международные и региональные протоколы и договоры, а также предпринять шаги по осуществлению приведенных в них мер.

2f. Укрепить потенциал правоохранительных органов
Необходимо выявить недостатки в правоохранительной и судебной системе и принять меры для повышения осведомленности, улучшения отчетности и успешного уголовного преследования. По возможности следует стремиться к организации международной подготовки кадров и обмену опытом, а также поощрять межсекторальную координацию и сотрудничество между отраслью и правоохранительными органами.

---

26. Например, нормативно-правовые акты, не дающие четкого представления о том, могут ли самостоятельно созданные сексуальные изображения, которыми обмениваются дети по взаимному согласию, считаться незаконными материалами по сексуальным надругательствам над детьми. Даже если дети не подвергаются судебному преследованию на практике, такая юридическая неопределенность с потенциальной криминализацией может подорвать их доверие, контроль и права на самостоятельность.

27. Под сексуальной эксплуатацией детей и жестоким обращением с ними (CSEA) подразумеваются случаи, когда ребенка принуждают или убеждают принять участие в сексуальных действиях. Речь может идти о физическом контакте или бесконтактных действиях, и такие действия могут происходить в Интернете или за его пределами.

3. Персональные данные и идентичность

3a. Создать или повысить эффективность существующих систем защиты данных с целью обеспечения особой защиты данных детей
Права детей в Интернете тесно связаны с тем, как собираются, хранятся и используются их данные. Законодательство и регулирование в области защиты данных детей должны быть доступными, эффективными и способными к эволюции в соответствии с возникающими рисками.[28] Это означает не только разработку нормативно-правового регулирования, но и обеспечение его практической эффективности и реализации.

3b. Установить протоколы и ограничения на использование технологий автоматизированного принятия решений, которые могут влиять на детей
Стандарты, законы и своды правил должны обеспечивать, чтобы дети могли пользоваться преимуществами автоматизированных систем и их права не ущемлялись вследствие автоматизированного принятия решений.[29] Особенно важно избегать потенциальной дискриминации. Такие протоколы и ограничения могут применяться, в частности, в контексте уголовного правосудия, социального обеспечения, здравоохранения, медицины, образования и частного сектора.

3c. Обеспечить надлежащую нормативно-правовую защиту биометрических данных детей
Правительству и регулирующим органам следует разработать соответствующие нормативно-правовые протоколы и ограничения в отношении использования биометрических данных детей с учетом их прав, целевых ограничений и требований политики обеспечения безопасности детей в Интернете.

3d. Создать четкое руководство, законы и нормативные акты в отношении практики, которая может повлиять на свободу действий детей
Создать правовые рамки, предотвращающие персонализированный таргетинг и отслеживание детей на основе их персональных данных в рекламных целях. Разработать правила использования систем предоставления рекомендаций и других автоматизированных процессов принятия решений или технологий, которые могут влиять на поведение детей, формировать их предпочтения и мнения, подрывать репутацию или ограничивать их опыт использования.[30]

3e. Обеспечить эффективный надзор и контроль
Создание органов и систем, которые могут собирать информацию, касающуюся безопасности детей в Интернете, и обеспечивать прозрачность и эффективное осуществление прав и защиты детей со стороны бизнеса, правительства и других организаций.

3f. Создать механизмы для обеспечения прозрачности
Надзор должен осуществляться назначенным регулирующим органом, обладающим достаточными ресурсами, необходимым потенциалом и компетенцией для понимания используемых систем и их влияния на права детей. Надзорный орган должен также иметь доступ к независимым исследованиям и экспертным знаниям.

4 Системы реагирования и поддержки

4a. Уведомление о контенте и его удаление
Государственные учреждения должны сотрудничать с экспертами, правоохранительными органами и представителями отрасли в целях создания и мониторинга эффективных протоколов уведомления о незаконных и вредных материалах, а также их удаления. Среди прочего, это потребует разработки протоколов и законодательства, позволяющего местным интернет-провайдерам ограничивать доступ к хостам, которые не удаляют подозрительный контент или постоянно нарушают законы или другие нормативные требования в отношении безопасности детей в Интернете.

4b. Установить процессы управления рисками для правонарушений в сфере сексуальной эксплуатации детей и жестокого обращения с ними (CSEA)
Следует наладить эффективный процесс управления правонарушителями с участием многих заинтересованных сторон и опорой на передовые международные стандарты. Правоохранители и другие сотрудники системы уголовного правосудия должны пройти подготовку по выявлению и расследованию противоправных действий. Управление рисками нарушителей в этой сфере является важным компонентом концепции безопасности детей в Интернете, поскольку от отдельных лиц или групп правонарушителей в Интернете может пострадать большое число детей.

---

28. Общий регламент о защите данных, Европейский союз, 2018 г.
29. «Мир скатывается в антиутопию цифрового благоденствия», предупреждение эксперта ООН по правам человека, Управление Верховного комиссара Организации Объединенных Наций по правам человека, 2019 г.
30. См., например, Иск об утечке данных в YouTube, «Макканн против Google», 2021 г.

4c. Предоставить достаточное количество ресурсов для оказания психосоциальной поддержки детям, ставшим непосредственными и косвенными жертвами преступлений, и членам их семей
Организации, обучающие специалистов в области психического здоровья, психологии и социальной работы, которые работают с уязвимыми детьми, должны иметь базовое представление о вопросах безопасности детей в Интернете.[31] Эта проблема должна быть интегрирована в более широкие системы безопасности и защиты детей, такие как охрана прав в школах или насилие в отношении детей (VAC).

4d. Создать механизмы выявления и защиты жертв
Одной из ключевых целей в деле предотвращения вреда, причиняемого в Интернете, является учет потребностей уязвимых детей и оптимальных способов их поддержки. Центры «одного окна» выступают в качестве первоначального комплексного учреждения для жертв насилия, обеспечивая доступ к целому ряду основных услуг — от медицинской до юридической помощи — из одного места. Такие центры закладывают основу для процедур защиты детей, оказывают поддержку жертвам и оперативно передают сообщения о преступлениях, совершаемых в Интернете, соответствующим органам.[32]

4e. Создать механизмы, не криминализирующие детей
Важно создать надлежащие механизмы для работы с детьми, нарушившими законы, связанные с безопасностью детей в Интернете, например в случаях кибербуллинга, распространения вредоносной информации или взлома. Дети должны быть по возможности исключены из системы уголовного судопроизводства. Следует отдавать предпочтение возможностям консультирования или восстановительного правосудия. Важно также убедиться, что в расчет принимаются все обстоятельства ребенка. Например, поведение ребенка может быть результатом буллинга, домогательств или иной формы принуждения.

5 Предпринимательская деятельность и права ребенка:

5a. Внедрить принципы встроенной безопасности, прав и этики
Необходимо создать стандарты и своды правил, требующие от разработчиков продукции, производителей и поставщиков услуг соблюдать права детей и содействовать обеспечению безопасности и защиты детей в Интернете. Условия использования должны отвечать наилучшим интересам ребенка. в частности, стандарты и своды правил должны препятствовать предоставлению детям вредного или неподходящего для них контента или контактов; защищать конфиденциальность детей в Интернете на уровне системы или устройства; а также решать проблемы безопасности, возникающие в связи с Интернетом вещей (игрушками с выходом в Интернет и сервисами потоковой передачи). Они должны обязывать частные компании проводить оценку воздействия на права детей для учета рисков и смягчения последствий, направленную на предложение услуг, соответствующих возрасту.

5b. Ввести минимальные стандарты[33]
Отрасль несет ответственность за защиту детей в цифровой среде. Речь идет о создании безопасного и доступного для детей онлайн-пространства, а не только о предотвращении доступа к вредному контенту. На этапе создания онлайн-сервисов предприятия обязаны демонстрировать, какие процедуры и особые меры приняты для обеспечения безопасности детей и соблюдения их[34] прав, используя систему оценки рисков.[35] Свод правил должен быть разработан ведущим министерством или другим ведомством под надзором Руководящего комитета. Стандарты должны носить обязательный характер.

5c. Использовать возрастную классификацию
Использование единой возрастной классификации для коммерческого контента, средств массовой информации, игр и другой деятельности в Интернете обеспечивает прозрачный и эффективный подход к управлению информационными продуктами и сервисами, воздействующими на детей. Она может распространяться на связанные с детьми товары и услуги, а также контент, предназначенный для разных возрастных категорий. Для запрещенного контента или деятельности, не подходящей для ребенка, необходимо вводить ограничения по возрасту или создавать пространство только для взрослых. в частности, речь идет о контентной фильтрации, направленной на блокировку нежелательных материалов.[36]

---

31. Эффективные методы предотвращения насилия против женщин и девочек: обзор доказательств, статья 3 «Механизмы реагирования для предупреждения насилия», What Works, 2015 г. стр. 28.
32. Предотвращение сексуальной эксплуатации детей и жестокого обращение с ними (CSEA): Модель национального реагирования, Глобальный альянс WeProtect, 2016 г.
33. См., например, Добровольные принципы противодействия сексуальной эксплуатации детей и жестокому обращению с ними в Интернете, GOV.UK, 2020 г.
34. См. раздел «Смягчение рисков и вреда».
35. Оценка воздействия на права детей, Детский фонд Организации Объединенных Наций, 2013 г.
36. Откуда они знают, что речь идет о детях?, Фонд 5Rights, 2021 г.

5d. Внедрить системы модерации и отчетности.
Поставщикам услуг необходимы механизмы для выявления тревожного или неподходящего контента, а также прозрачные и надежные системы мониторинга для всех онлайн-сервисов, включая механизмы удаления. Для сообщения о нарушениях и получения доступа к специализированной поддержке и консультациям должна работать горячая линия. Механизмы отчетности должны быть легкодоступными для детей. в качестве дополнительного инструмента следует рассмотреть системы сообщения о нарушениях.

5e. Обеспечить защиту детей от коммерческого давления
Меры по защите детей от коммерческого давления должны включать поощрение проектов, учитывающих возрастные ограничения; предотвращение таргетированной рекламы и передачи информации третьим сторонам; а также повышение осведомленности об условиях, в которых растут дети. Продукты и услуги, которые учитывают права и повышают безопасность детей в Интернете, могут быть сертифицированы, а в отношении разработчиков, нарушающих эти принципы, могут быть приняты соответствующие меры.

5f. Обеспечить внедрение стандартов, учитывающих интересы детей, для минимизации рисков, связанных с безопасностью ребенка в Интернете
Например, речь идет о возможных контактах взрослых незнакомцев с детьми, таргетированной рекламе азартных игр или рекомендациях вредного контента. Принципы безопасности детей в Интернете должны быть внедрены на этапе проектирования, чтобы предотвратить дальнейшие потенциальные проблемы.

6 Обучение

6a. Обеспечить обучение, развитие навыков и подготовку для всех, кто связан с безопасностью детей в Интернете
Все участники правоохранительной системы и специалисты, работающие с детьми в таких сферах, как образование и здравоохранение: от сотрудников экстренных служб до судей, — должны быть осведомлены о безопасности детей в Интернете. Необходимо провести для них всестороннее обучение, в том числе по вопросам о том, как безопасность детей в Интернете связана с их конкретными обязанностями, как определить противоправное поведение и предоставить помощь жертвам.

6b. Провести специализированное обучение по вопросу психосоциальной поддержки и выявлению всего спектра проблем, связанных с безопасностью детей в Интернете
Чтобы выполнять свои обязанности эффективным образом, специалисты-практики должны проходить обучение по вопросам безопасности детей в Интернете, политики, обеспечивающей защиту детей, а также консультирования детей и семей. Вопросы безопасности ребенка в Интернете должны быть включены в существующие программы в области защиты детей. Специалисты, работающие с детьми в образовательных, медицинских, общественных и других учреждениях, должны научиться распознавать признаки и симптомы проблем, связанных с безопасностью в Интернете.

6c. Создать обучающие программы в системе высшего специального образования
Занятия по вопросам безопасности детей в Интернете должны стать обязательной частью учебных программ государственных и частных университетов или других учебных заведений, готовящих учителей, медицинских работников, психологов и других специалистов. Необходимо проводить регулярную оценку эффективности этого обучения с учетом новой информации и проблем, связанных с безопасностью детей в Интернете. Учебные планы должны охватывать все аспекты безопасности детей в Интернете, как указано в настоящей политике.

6d. Поощрять профессиональное развитие
Чтобы идти в ногу с новыми технологиями и устранять препятствия и проблемы по мере их появления, программы непрерывного обучения по вопросам безопасности детей в Интернете для специалистов в соответствующих областях должны регулярно пересматриваться и обновляться.

7 Образовательные программы

7a. Назначить ведущего специалиста по охране прав детей
Каждая школа должна назначить ведущего специалиста по охране прав детей.[37] Таким специалистам необходимо пройти обучение в области процедур защиты детей и безопасности детей в Интернете. Ведущие специалисты будут нести ответственность за принятие, введение в действие и применение в школах правил безопасности детей в Интернете (включая процедуры безопасности и анонимного сообщения о нарушениях). Также они должны выступать в качестве контактных лиц по вопросам, касающимся защиты детей и их безопасности в Интернете, и передавать сообщения о причиненном вреде соответствующим органам. Кроме того, ведущим специалистам следует содействовать осуществлению планов мероприятий, направленных на защиту детей от любого вреда.

37. В качестве специалиста могут выступать участники школьного комитета по безопасности, педагог или представитель местного комитета по защите детей, в котором представлены школы.

7b. Содействовать развитию доступного цифрового образования
Необходимо продвигать контент, в том числе программы для сверстников, направленный на развитие цифровых навыков и расширение возможностей детей в создании сообществ, в которых действует атмосфера взаимного уважения и поддерживается безопасность детей в Интернете. Комплексная программа цифрового образования должна охватывать темы, связанные с данными и цифровой грамотностью, наряду с такими вопросами, как сексуальная жизнь и согласие. Необходимо также обеспечить обучение родителей/опекунов, чтобы они могли успешно следить за безопасностью их ребенка в Интернете.

7c. Продвигать образовательный контент
По мере распространения цифровых технологий ученики и учителя должны обучаться необходимым навыкам взаимодействия с цифровыми системами, чтобы пользоваться всеми преимуществами учебных программ как на местном, так и на иностранных языках.

7d. Повышать осведомленность по вопросам данных
В школьный учебный план должны быть введена программа обучения по вопросам данных. в рамках этой программы дети получат знания о том, как может быть использована их информация, и базовое понимание экономики данных. Ее цели — продвигать позитивное, автономное и творческое использование цифровых технологий детьми; четко определить риски, выгоды и социальные результаты использования таких технологий; а также обеспечить широкое распространение, понимание и применение защитных и профилактических мер в этой сфере. Обучение по вопросам данных должно четко определять круг заинтересованных сторон, отвечающих за безопасность в Интернете.

7e. Поощрять критическое мышление
Обучение критическому мышлению и повышение осведомленности о рисках, связанных с дезинформацией в Интернете, должны быть включены в образовательные программы в области компьютерной грамотности. Такое обучение должно включать вопросы прав человека, в частности, прав ребенка, и то, как они применяются в Интернете и в реальной жизни.[38]

7f. Ввести в школах формальные процедуры обеспечения безопасности детей в Интернете
Подготовка по вопросам безопасности детей в Интернете должна составлять обязательную часть педагогического образования как на уровне начальной, так и средней школы, а также стать одним из основных направлений непрерывного обучения учителей без отрыва от основной работы. Все учителя должны пройти обязательное обучение в области безопасности детей в Интернете, ознакомиться со школьной политикой в этом отношении и проводить на эту тему занятия для учеников. Чтобы следить за соблюдением стандартов и школьной политики в отношении безопасности детей в Интернете, школы должны назначить ведущего специалиста в этой области.

8 Связи с общественностью и формирование коллективной сознательности

8a. Разработать программу повышения осведомленности
Стратегии повышения осведомленности помогут людям понять проблему безопасности детей в Интернете и ориентироваться в ней, продолжая при этом пользоваться преимуществами цифрового пространства. в подготавливаемых материалах должны быть четко изложены принципы безопасности детей в Интернете и действия, которые могут быть предприняты для понимания риска, снижения вреда, сообщения о правонарушениях и требования возмещения. Данная информация будет представлена в простой форме на официальных сайтах. Целевые сообщения и материалы должны разрабатываться на основе консультаций с детьми, молодежью и родителями/опекунами. в них следует учитывать особые потребности родителей/опекунов и детей, уделяя особое внимание самым маленьким и наиболее уязвимым детям, включая детей с особыми образовательными потребностями или без родительского попечения. Метод обучения «равный равному» является ценной стратегией для детей всех возрастов, позволяющей им ознакомиться со своими правами и обязанностями в Интернете. Эта программа публично распространяемых сообщений поможет детям и взрослым понять проблемы и сделать разумный выбор в отношении их взаимодействия в Интернете, но не заменяет официальное образование, профессиональную подготовку, принцип встроенной безопасности или программу корпоративной ответственности. Такая информация должна охватывать весь спектр вопросов безопасности детей в Интернете, как указано в настоящей политике.

38. См. статью 29 Конвенции о правах ребенка и соответствующие разделы Замечания общего порядка.

Пять межсекторальных вопросов
1. Как выявлять риски и смягчать их последствия
2. Как обеспечить доступ к информационным технологиям, доступность информации и взаимодействие всех заинтересованных сторон
3. Как построить цепочку ответственности и сотрудничества
4. Как добиться того, чтобы проект учитывал интересы детей
5. Как обеспечить эффективность системы

Десять областей применения политики
1. Возможности вовлеченных организаций
2. Нормативно-правовое регулирование
3. Персональные данные, идентичность и самостоятельность
4. Системы реагирования и поддержки
5. Корпоративная ответственность
6. Обучение
7. Образовательные программы
8. Связи с общественностью и формирование коллективной сознательности
9. Научно-исследовательская работа
10. Международное сотрудничество

8b. Предоставить доступную информацию и учебные материалы
Обучение по вопросам безопасности в Интернете должно начинаться в раннем детстве и развиваться в соответствии с меняющимися потребностями ребенка по мере его взросления: необходимо подготовить специальные руководства для детей всех возрастов, их семей и лиц, осуществляющих уход. Информационные материалы должны продвигать позитивное использование цифровых технологий, учитывать вопросы сексуальности и согласия, а также потребности всех детей, независимо от гендера, возраста, дохода или происхождения. Информация, предоставляемая третьими сторонами, должна отражать принципы защиты детей и помогать ребенку любого возраста узнавать о рисках и своих правах в Интернете. в материалах необходимо подчеркивать мысль о том, что дети и пользователи не несут ответственности за плохие вещи, которые с ними происходят. Группы по интересам, молодежные клубы, семьи, религиозные учреждения и цифровые платформы будут играть важную роль в эффективном повышении осведомленности о безопасности детей в Интернете и неофициальном обучении на уровне сообщества.

8c. Повысить осведомленность о безопасности детей в Интернете в средствах массовой информации
Следует предоставить средствам массовой информации материалы по вопросам безопасности детей в Интернете для их освещения в удобной для детей форме. СМИ и развлекательные компании должны быть осведомлены о безопасности детей в Интернете. Кроме того, где это уместно, их необходимо поощрять к оказанию сбалансированной, ответственной и содержательной поддержки кампаниям по повышению осведомленности общественности. Необходимо поощрять публикации по всему спектру вопросов безопасности детей в Интернете, а не только наиболее драматичные заголовки, связанные с этим.

8d. Привлекать родителей/опекунов и детей к обсуждению вопросов безопасности детей в Интернете
Родители/опекуны и другие члены семьи должны иметь возможность понимать и принимать меры по обеспечению безопасности детей в Интернете в собственном доме. Для эффективного выявления проблем, поиска решений и путей повышения осведомленности о безопасности детей в Интернете необходимо провести консультации с семьями и детьми.

9. Научно-исследовательская работа

9a. Создать программы исследований в области безопасности детей в Интернете
Странам следует учредить центральный научно-исследовательский фонд для разработки научно-исследовательской программы с четко поставленными и актуальными задачами и целями, чтобы обеспечить возможность проведения непрерывных исследований по широкому кругу вопросов безопасности детей в Интернете. Там, где возможно, странам следует поддерживать контакты и сотрудничать друг с другом в области научно-исследовательской работы по вопросам безопасности детей в Интернете. Анализ пробелов призван обеспечить приоритетное выделение ресурсов в областях, в которых ощущается наибольшая потребность, и избежать дублирования исследований. Доступ к исследованиям должен предоставляться региональным или международным партнерам, особенно тем из них, которые располагают наименьшими ресурсами.

9b. Постоянно внедрять инновации
Научные данные будут использоваться при разработке продуктов и услуг со встроенной безопасностью; позволят оценить практическое применение стратегии в отношении безопасности детей в Интернете; а также обеспечат понимание опыта взаимодействия детей с Интернетом и связанных с ним решений в национальном контексте.

9c. Учредить эффективные научно-исследовательские центры по вопросам безопасности детей в Интернете
В рамках существующих учреждений (университетов, медицинских учреждений, центров инноваций) странам следует создать центры передового опыта, которые могли бы обмениваться знаниями об инструментах и услугах, связанных с безопасностью детей в Интернете, и сотрудничать в этой области на национальном, региональном и международном уровнях.

9d. Создать четкие этические рамки для научно-исследовательской работы в области безопасности детей в Интернете[39]
Странам следует разработать руководящие принципы для исследователей, занимающихся вопросами безопасности детей в Интернете, включая эффективное включение прав детей в рамки исследовательского процесса. Речь идет о четких инструкциях по сбору данных детей и учете этических и правовых последствий их обработки. Интересы ребенка должны в первую очередь учитываться при создании этических рамок для научно-исследовательской работы по вопросам безопасности детей в Интернете, в том числе в ситуациях, связанных с доступом к информации в общественных интересах.

9e. Создать нормы, регулирующие сбор информации
Регулирующим органам, занимающимся вопросами безопасности детей в Интернете, следует создать механизмы сбора информации, которые позволят им осуществлять мониторинг и оценку эффективности мер по обеспечению безопасности детей в Интернете в различных контекстах и их воздействия на различные группы детей. Мониторинг и оценка мер в этой сфере должны стать частью научно-исследовательской работы.

9f. Обеспечить доступ к данным частных компаний в общественных интересах
Необходимо создать механизмы, в рамках которых социальные сети и другие компании будут делиться своими данными для поддержки исследований с соблюдением наилучших интересов ребенка.

9g. Обеспечить актуальность данных и статистики в конкретных условиях
Для поддержания уровня понимания национальных проблем и адекватного на них реагирования статистические модели должны отражать местную картину и позволять осуществление мониторинга трансграничного воздействия.

10. Международное сотрудничество

10a. Установить официальные рамки взаимодействия (например, заключить меморандумы о взаимопонимании) с региональными и глобальными сообществами по безопасности детей в Интернете
Укрепление международного сотрудничества в целях повышения безопасности детей в Интернете во всем мире имеет решающее значение для обеспечения глобальной безопасности. Странам следует официально закрепить сотрудничество для совместных государственно-частных инвестиций в областях, связанных, в том числе, с кибербезопасностью, наращиванием потенциала для обеспечения безопасности детей в Интернете, инновациями, правоохранительной деятельностью, системой правосудия, образования и т. д.

10b. Стать участником региональных и международных правовых инструментов, поощряющих сотрудничество по вопросам защиты детей в Интернете
Странам следует определить ключевые региональные и международные инструменты, которые позволят им сотрудничать с другими странами по вопросам безопасности детей в Интернете. Они должны включать, среди прочего: международные соглашения о сотрудничестве между правоохранительными органами; передовую международную практику; программы, которые могут обеспечить ресурсы для сотрудничества по вопросам безопасности детей в Интернете; а также доступ ко всем правам человека или связанным с ними стандартам, которые будут способствовать сотрудничеству между странами.

10c. Определить страны и организации-партнеры, которые могут предоставить соответствующие модели и поддержку для повышения безопасности детей в Интернете
В некоторых случаях нет необходимости разрабатывать политику с нуля. Странам следует определить соответствующие примеры концепций обеспечения безопасности детей в Интернете, которые могут быть использованы и адаптированы к конкретным условиям. Обмен информацией о проблемах и трудностях, связанных с безопасностью детей в Интернете, может быть весьма полезным для планирования, разработки и осуществления политики.

39. Дети и жизненный цикл данных: права и этика в мире больших данных, Детский фонд Организации Объединенных Наций, 2017 г.

10d. Поддерживать другие страны, разрабатывающие политику безопасности детей в Интернете
По возможности, важно делиться информацией о типовых законах, нормативных рамках, извлеченных уроках и прочими материалами, которые могут быть использованы другими странами для разработки собственной концепции и политики в области безопасности детей в Интернете.[40]

40. См., например, материалы по международному лидерству и сотрудничеству, подготовленные комиссаром по электронной безопасности Австралии, 2021 г.

5RIGHTS FOUNDATION

End Violence Against Children