CENTER FOR GLOBAL IT-COOPERATION

АНАЛИТИЧЕСКИЙ ОБЗОР

МЕЖДУНАРОДНАЯ ПРАКТИКА В ОБЛАСТИ ЗАЩИТЫ ДЕТЕЙ В ИНТЕРНЕТЕ

РЕЦЕНЗЕНТЫ:

АГЕЕВ А.И.,
Директор Института экономических стратегий РАН (ИНЭС), генеральный директор Международного научно•исследовательского института проблем управления (МНИИПУ), директор Международного института Питирима Сорокина — Николая Кондратьева, президент Международной академии исследований будущего, д.экон.н., профессор

СУТЫРИНА А.С.,
Директор Института правового регулирования Национального исследовательского университета «Высшая школа экономики», кандидат юридических наук

Аннотация

Центром глобальной ИТ-кооперации (Center for Global IT-Cooperation, CGITC, https://cgitc.ru) представлен аналитический обзор зарубежных подходов к проблеме защиты детей в цифровом пространстве. Информация основана на аналитических исследованиях, обзорных публикациях, инструментах «мягкого права», нормативно-правовых актах, материалах общественных дискуссий в зарубежных странах. Обзор дает базовые представления о магистральных тенденциях в этой сфере и может служить для разработки современных инструментов регулирования на национальном уровне.

Представленную в обзоре информацию в составе других экспертных документов возможно использовать при формировании позиции о необходимости разработки в стране дополнительных нормативно-правовых актов. Материал также может быть изучен различными организациями и компаниями для знакомства с зарубежным опытом в области защиты детей в цифровой среде и принятия управленческих решений. Важно отметить, что при выработке такого рода решений и регуляторных мер должны быть комплексно использованы фактические научные и исследовательские материалы, статистические данные и практический опыт, накопленный в профильных ведомствах и организациях, непосредственно отвечающих за вопросы безопасности в Интернете и национальном информационном пространстве.

АВТОРЫ

Игнатьев А.Г., руководитель аналитического направления CGITC;
Курбатова Т.А., старший аналитик CGITC.

Корректор: Нагель Е.В.

АНО «Центр компетенций по глобальной ИТ-кооперации» создан в 2020 году для экспертного изучения вопросов международного сотрудничества в сфере информационных технологий (ИТ), укрепления позиций России в глобальной ИТ-кооперации, а также продвижения новых подходов к многостороннему управлению Интернетом.

CGITC является членом Сектора развития электросвязи (ITU-D) Международного союза электросвязи, участником международного Форума по управлению интернетом (IGF), соорганизатором ежегодного Российского форума по управлению интернетом.

Центр проводит исследования и реализует проекты в области цифровой грамотности, управления Интернетом, научно-технического сотрудничества в сфере цифровой экономики, оказывает практическое содействие новым командам и начинающим экспертам по продвижению инноваций и стартапов. Во взаимодействии с международным сообществом и при поддержке заинтересованных специалистов в России CGITC на регулярной основе проводит ряд научных и экспертных круглых столов, конференций и вебинаров.

В 2022 году CGITC выступил ключевым организатором ежегодного Молодежного российского форума по управлению интернетом, а также участвует в работе исследовательской сети Think20 «Группы двадцати».

ПРИСТУПАЯ К ОЗНАКОМЛЕНИЮ С ОБЗОРОМ, ВЫ ПОДТВЕРЖДАЕТЕ СВОЕ СОГЛАСИЕ С НИЗЛОЖЕННЫМИ НИЖЕ УСЛОВИЯМИ:

— Правообладатель не несет ответственность за использование информации, содержащейся в обзоре.

— Обзор носит исключительно информационный характер и составлен на основе открытых источников, признанных надежными, однако правообладатель не несет ответственность за точность приведенных данных.

— Выводы, представленные в обзоре, также имеют исключительно информационный характер и основаны на информации, полученной из открытых материалов, указанных в списке использованных источников.

— Обзор не является юридическим заключением по вопросам, рассмотренным в нем. Правообладатель не несет ответственности за решения, принятые на основании представленных в обзоре данных.

— Обзор также включает в себя ссылки на сторонние веб-сайты, находящиеся вне контроля правообладателя. Поэтому он не несет ответственность за их содержание — такая ответственность возлагается на представителей сторонних веб-сайтов.

Оглавление

ВВЕДЕНИЕ

ЦЕЛИ И ОХВАТ ИССЛЕДОВАНИЯ

Центром глобальной ИТ-кооперации (Center for Global IT-Cooperation, CGITC) подготовлен аналитический обзор зарубежных подходов к проблеме защиты детей в цифровом пространстве. Информация основана на аналитических исследованиях, обзорных публикациях, инструментах «мягкого права», нормативно-правовых актах, материалах общественных дискуссий в зарубежных странах. Обзор дает базовые представления о магистральных тенденциях в этой сфере за рубежом и может служить для анализа и возможной разработки современных инструментов регулирования на национальном уровне.

В материале представлены практики и инструменты следующих международных организаций: ООН и учреждений системы ООН (UNESCO, UNICEF, UNIAWG-VAC, Комитета ООН по правам ребенка), ITU, IGF, ILO, OECD, Interpol, CoE. Отражены значимые программы и меры по защите детей в разных странах — Великобритании, Греции, Индии, Ирландии, Сербии, США и Европейского союза. Освещена деятельность Ассоциации стандартов Института инженеров по электронике (IEEE), Европейской инициативы «Безопасность онлайн» (European Save Online Initiative), альянса iKeepSafe, Международной линии помощи детям (Child Helpline International), Фонда наблюдения за интернетом (IWF), Глобального альянса WeProtect и других. Рассмотрены роль и активность онлайн-платформ и цифровых сервисов: ESET, Google, Facebook, Instagram, Mozilla, TikTok — в обеспечении безопасности детей в Сети.

В обзоре приведены основные риски для несовершеннолетних в Интернете.

В приложениях содержатся материалы с дополнительной полезной информацией в рамках освещаемой тематики. В заключительной части выделяются преобладающие зарубежные подходы в контексте рассмотренного международного опыта, а также предлагаются практические рекомендации для возможного использования в деятельности российских государственных органов, бизнес-ассоциаций, общественных организаций и других площадок, в том числе при международном взаимодействии в рамках Евразийского экономического союза, BRICS и других объединений.

АКТУАЛЬНОСТЬ ПРОБЛЕМАТИКИ

Через Интернет дети могут реализовать свои возможности и права, в том числе право на самовыражение, доступ к информации, мирное общение, защиту ото всех форм насилия. Вместе с тем цифровая среда и прорывные цифровые технологии несут в себе и новые риски для детской аудитории, что требует принятия адекватных мер защиты и повышения уровня информированности детей и родителей.

Международные проекты и инициативы в области защиты несовершеннолетних основаны на приверженности Целям в области устойчивого развития ООН, а именно Цели № 4 (цифровые навыки), Цели № 5 (гендерное равенство), Цели № 10 (сокращение неравенства), Цели № 16.2 (искоренение жестокого обращения с детьми и насилия над ними) и Цели № 17 (активизация работы в рамках глобального партнерства по устойчивому развитию). Для достижения указанных целей заинтересованные лица стремятся обучать детей безопасному взаимодействию с Интернетом и внедряют различные практики, помогающие усилить надежное использование цифровых технологий.

Неравенство в доступе к цифровым технологиям и информации подтверждает необходимость инвестирования в связь и дистанционное обучение, которые могут обеспечить каждому ребенку, особенно из наиболее уязвимых категорий, возможность погрузиться в широкий спектр образовательных возможностей. Многие молодые люди сегодня оторваны от цифровых решений, способных значительно улучшить их жизнь.

Вопросы развития детей и их участия в жизни общества являются сквозными темами Повестки дня ООН в области устойчивого развития на период до 2030 года. Поиск согласованных подходов правительствами, гражданским обществом и бизнесом возможен на основе многостороннего сотрудничества на самых разных уровнях. Тематика защиты детей в Интернете тесно сопряжена с задачами социальной безопасности, здравоохранения, повышения качества образования и услуг. Только комплексные решения на международном уровне способны обеспечить несовершеннолетним надлежащую защиту, возможность развиваться и реализовывать потенциал для достижения целей Повестки дня.

ПОНЯТИЯ, ИСПОЛЬЗУЕМЫЕ В ОБЗОРЕ

Определения, к которым прибегают наиболее влиятельные международные организации, такие как UNESCO, UNICEF, Еврокомиссия, ITU, CoE, как правило, ориентированы на граждан всех возрастов. Далее из их числа представлены основные понятия по тематике исследования.

Цифровые навыки. Владея ими, можно без труда использовать инновационные технологии во благо собственному развитию. Цифровые навыки включают в себя практические навыки, навыки навигации, социальные и творческие навыки, а также навыки работы с мобильными устройствами. Без них сегодняшние дети останутся далеки от перспектив новаторских компаний. Повышая уровень компетенции в цифровой среде, молодежь повышает возможности престижного трудоустройства в будущем: цифровизация всех сфер жизни создает огромный спрос на доходные рабочие места по всему миру.

Дети совершенствуют цифровые навыки участием в большом количестве онлайн-мероприятий. Но одновременно с приобретением полезного опыта таким образом несовершеннолетние становятся более уязвимыми к интернет-угрозам.

Цифровая грамотность. Это крайне важный навык для современных детей. Черпая знания об окружающем мире посредством новейших технологий и онлайн-образования, они стали уязвимой группой в интернет-пространстве. Исследования показывают, что несовершеннолетние с высоким уровнем цифровой грамотности с большей уверенностью познают онлайн-мир.

Дело в том, что возрастание онлайн-активности ведет к увеличению подверженности детей потенциальным рискам. Несовершеннолетние с более высоким уровнем цифровой грамотности лучше подготовлены к решению гипотетических проблемных ситуаций в Сети. Это делает их более устойчивыми к любым допустимым опасным последствиям.

В Пояснительных замечаниях общего порядка № 25 от 2021 года Комитета ООН по правам ребенка цифровая грамотность определяется как способность использовать информационные и коммуникационные технологии для поиска, оценки, развития, творчества и общения.

Согласно UNICEF, цифровая грамотность относится к знаниям и навыкам, которые позволяют детям оставаться благополучными в глобальном цифровом мире, обеспечивать свою безопасность и использовать возможности, соответствующие их возрасту, местной культуре и контексту.

Следует отметить, что из частично совпадающих с этим определением терминов наиболее часто встречаются «медиаграмотность», «информационная грамотность»

и «информационно-коммуникационные технологии». Согласно UNESCO, «цифровая грамотность» часто употребляется аналогично «информационной грамотности»

и подразумевает собой способность эффективно использовать доступ к информации, а после критически оценивать ее, применяя ряд инструментов, в том числе цифровых технологий, для обогащения уровня знаний.

UNICEF под медиаграмотностью предлагает рассматривать осознанное активное или пассивное использование средств массовой информации и их методов. Также в понятие вкладывается способность читать, анализировать и эффективно коммуницировать, прибегая к различным медийным форматам: телевидению, печати, радио или Интернету.

Экспертная группа Еврокомиссии по медиаграмотности определяет этот термин как набор «технических, когнитивных, социальных, гражданских и творческих способностей, которые позволяют гражданину получать доступ к медиа, критически понимать их и взаимодействовать с ними». Такие способности необходимы для участия в экономических, социальных и культурных аспектах жизни общества.

Цифровая гигиена. Также известна как кибергигиена или интернет-гигиена. Под этими определениями понимается набор принципов и практик, помогающих сохранять цифровую жизнь здоровой. Соблюдение цифровой гигиены повышает безопасность ребенка и уровень надежности его цифровых инструментов. При этом единого определения термина, согласованного на международном уровне, не существует.

Сексуальное насилие в Интернете. Сексуальный контент навязывается детям в Сети через чаты, электронные письма, социальные сети. К нему причисляются сексуализированное поведение перед веб-камерами, размещение эротических или порнографических фотографий и видео, использование сексуального языка и груминг.

За подобным могут последовать приглашения на тайные встречи с целью надругательства или эксплуатации. При этом злоумышленник может добиваться доверия ребенка постепенно, ис-

следуя его предпочтения в социальных сетях.

Кибербуллинг. UNICEF определяет его как издевательство с использованием цифровых технологий, которое может происходить в социальных сетях, платформах обмена сообщениями и игровых платформах. Это повторяющееся поведение направлено на то, чтобы напугать, разозлить или пристыдить мишень. В отличие от обычного буллинга, кибербуллинг оставляет цифровой след — запись, которая может оказаться полезной и предоставить доказательства для остановки злоупотребления.

ОСНОВНЫЕ РИСКИ ДЛЯ ДЕТЕЙ В ИНТЕРНЕТЕ

ОБЩАЯ КЛАССИФИКАЦИЯ И КАРТА РИСКОВ

В 2011 году Организация экономического сотрудничества (Organisation for Economic Co-operation and Development, OECD) приняла Типологию рисков в Интернете для детской аудитории. В документе были представлены обзор и классификация различных опасностей. С тех пор цифровая среда изменилась и риски значительно эволюционировали. В январе 2021 года OECD опубликовала Обновленную типологию рисков для детей в цифровой среде, в которой по-прежнему исследовались сетевые опасности, но также и то, как изменился их характер. Сегодня OECD выделяет четыре категории рисков:

- контентные;
- поведенческие;
- контактные;
- потребительские.

Кроме того, типология определяет сквозные опасности (таблица № 1). Они пересекаются с четырьмя приведенными категориями рисков и имеют широкий диапазон влияния на жизни детей. К таковым относятся риски:

- конфиденциальности;
- передовых технологий;
- для здоровья и благополучия.

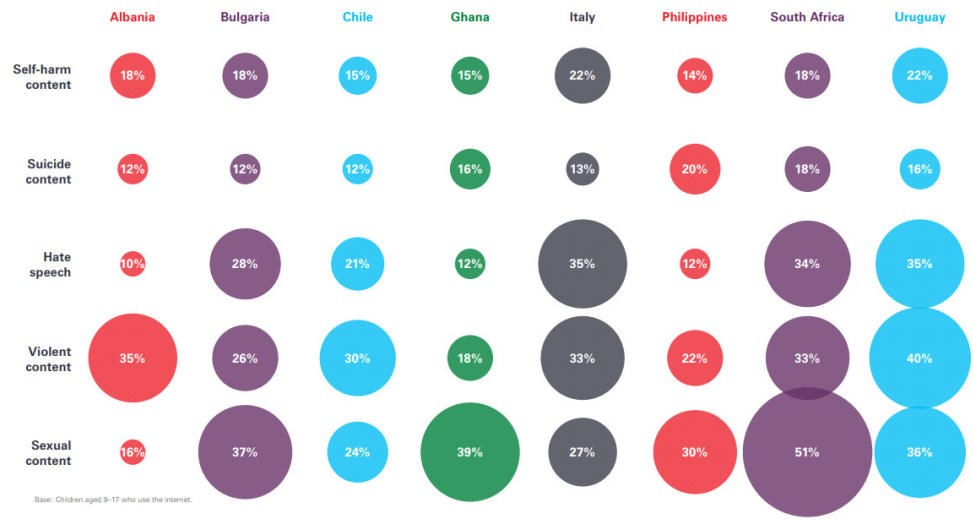
Таблица № 1. Риски для детей в цифровой среде

КАТЕГОРИИ	КОНТЕНТ	ПОВЕДЕНЧЕСКИЕ РИСКИ	КОНТАКТНЫЕ РИСКИ	ПОТРЕБИТЕЛЬСКИЕ РИСКИ
Сквозные риски	Защита частной жизни: межличностные, институциональные и коммерческие			
	Передовые технологии, например «Интернет вещей», прогнозная аналитика, биометрия			
	Здоровье и благополучие			
Проявления рисков	Ненавистнический контент	Ненавистническое поведение	Ненавистнические нападки	Маркетинговые риски
	Вредоносный контент	Вредоносное поведение	Вредоносные нападки	—
	Неправомерный контент	Неправомерное поведение	Неправомерные нападки	Финансовые риски
	Дезинформация	Проблемное поведение, инициированное пользователем	Другие проблемные нападки	Риски для безопасности

Источник: OECD, Типология рисков в Интернете для детской аудитории

Исследование UNICEF показывает, что в разных странах градация рисков значительно различается (рисунок № 1). Кроме того, степень наносимого ими вреда зависит от психологической устой-

Рисунок № 1



Источник: UNICEF, «Взросление в связанном мире»

чивости детей, а также от поддержки и цифровых навыков взрослых, в том числе от умения управлять настройками конфиденциальности.

Несовершеннолетние сталкиваются с теми же проблемами безопасности, что и взрослые, — со ссылками на вредоносные сайты, вредоносными программными обеспечениями. Однако есть способы, которые используются только в отношении детей. Среди таковых — перенаправление на «фан-сайты», содержащие вредоносные данные, поддельные сообщения от друзей, предложения «бесплатной» музыки, фильмов или чего-то другого, что вызовет у ребенка соблазн кликнуть.

Несложная локализация сетевых ресурсов для детей: образовательных программ, учебных материалов, развлекательного контента, игр, кино, мультфильмов — позволяет злоумышленникам легко получать персональные данные несовершеннолетних, прицельно воздействовать на конкретную возрастную категорию.

В отчете Совета Великобритании по безопасности детей в Интернете сделан вывод о том, что дети, как правило, позитивно относятся к своему онлайн-опыту. При этом набор используемых ими услуг не всегда предполагает защиту по возрасту и потребностям.

Ниже разобраны наиболее характерные риски для детской онлайн-безопасности:

Кибербуллинг. Как свидетельствуют данные американского ресурса SafeWise, который анализирует тенденции в области онлайн-безопасности, девочки чаще становятся его жертвами и все больше мальчиков признаются в издевательствах над другими детьми в Интернете. В процессе обмена личной информацией в Сети можно столкнуться со следующими проявлениями кибербуллинга:

— оскорбительными веб-страницами, фото, видео и комментариями, в том числе о расе или религии;

— онлайн-слухами;

— угрозами причинения боли в сообщениях;

— комментариями с сексуальным подтекстом;

— попытками выдать себя за другого человека с целью травли.

Негативный и деструктивный контент. Одна из наиболее распространенных онлайн-угроз включает в себя как грубости, вульгарный язык и язык вражды, так и сексуализированные изображения и может оказать крайне отрицательное воздействие на впечатлительного ребенка. Ресурс SafeWise заявляет, что в 2018 году более 55 % детей от 10 до 12 лет подвергались воздействию насильственного контента в Интернете и почти 60 % — сталкивались с сексуализированными словами или изображениями.

Язык вражды — это языковые средства, оскорбляющие человека или группы людей по расовому, этническому, гендерному или религиозному признаку, а также по состоянию здоровья. На бытовом уровне это в первую очередь показатель культуры социума.

На официальном уровне такого рода высказывания недопустимы и в совершенстве должны быть наказуемы.

Контент сексуального характера, сексуальное онлайн-насилие. Основная проблема здесь заключается в том, что опасные для несовершеннолетних материалы и практики не всегда можно приравнять к преследуемым законом преступлениям. Злоумышленники используют уловки, которые затрудняют действия правоохранителей по их пресечению и последующему наказанию на основе нормативных актов. Отдельные сложности также связаны с выявлением такого рода материалов и инцидентов в Сети.

Отчет компании NetClean «О преступлениях, связанных с сексуальным насилием в отношении детей в 2019 году» выявил, что сексуализированные материалы распространялись как добровольно, так и принудительно, посредством груминга или сексуального вымогательства. При этом как жертвы, так и провокаторы сексуального насилия над детьми в прямом эфире были в основном из США и Европы. Пострадавшие из удаленных прямых трансляций — в основном из Азии (большинство с Филиппин), а также из Европы, России и США.

Онлайн-хищники. Интернет — одна из самых быстрорастущих арен для торговли детьми и их сексуальной эксплуатации. Преступники, именуемые онлайн-хищниками, все чаще пользуются современными технологиями на всех этапах злодеяния — для привлечения, сексуальной эксплуатации жертв и контроля над ними. Легко получив с веб-сайта образовательных учреждений конфиденциальную информацию о несовершеннолетних вроде имени и контактных данных, злоумышленники пытаются наладить с ними контакт, в том числе предлагая советы по построению карьеры.

Дипфейки. Одно из самых популярных занятий

детей — монтировать клипы о себе и размещать их в социальных сетях: Facebook, Instagram, Snapchat, TikTok. Загружая свои фото или видео для обработки, несовершеннолетние предоставляют их третьим лицам, неосознанно способствуют созданию обширных библиотек контента.

Отмечаются случаи, когда из материалов детей с помощью нейросетей создаются всевозможные дипфейки (реалистичные подмены лиц или других частей тела) сексуального характера. К серьезной проблеме в расследовании подобных инцидентов относят сложности с идентификацией фигурирующих в роликах несовершеннолетних. Дипфейк, как правило, скрывает настоящее лицо ребенка, подвергшегося насилию, а не установив жертву, весьма сложно выйти на преступника. Также существует риск зря потраченного времени на поиск несовершеннолетнего, который на самом деле не перенес сексуального надругательства.

Риски, сопряженные с игровой практикой. С развитием индустрии интерактивных развлечений дети становятся все более вовлечены в игровые активности, уделяют им все больше времени. Во многих случаях применительно к играм можно вести речь о гемблинге. В Большом юридическом словаре этот термин раскрывается как «организация азартных игр, вид преступного промысла». Похожее определение дано и в Энциклопедическом словаре по психологии и педагогике: «гемблинг — игромания, патологическое пристрастие к азартным играм».

Говоря о рисках для игроков, нельзя не упомянуть о формировании онлайн-зависимости. Всемирная организация здравоохранения в 2019 году проголосовала за принятие последнего издания Международной классификации болезней, включив в него запись об игровом расстройстве как о поведенческой зависимости. При этом, по данным американского Исследовательского центра Pew Research Center, 97 % мальчиков-подростков и 83 % девочек играют в игры на тех или иных устройствах.

В современных играх зачастую присутствуют различные лотереи и лутбоксы, которые провоцируют игроков делать ставки, рисковать, приобщаться к атмосфере азарта. Кроме того, возможны и случаи грубой манипуляции и принуждения, подталкивающие осуществлять оплату различных виртуальных атрибутов для продвижения в игре. Проблема осложняется еще и тем, что сейчас в мире только начали возникать эффективные подходы к регулированию онлайн-гемблинга. Также широкие возможности моделирования игровых ситуаций позволяют формировать у игроков те или иные пристрастия и представления о мире. Кроме того, в ходе игры нередко происходит ознакомление с материалами, угрожающими здоровью или включающими в себя деструктивный или противоправный контент. При этом достаточно сложно обеспечить всестороннюю модерацию на всех этапах игры.

Игровые учетные записи постоянно подвергаются взлому: хакеры крадут данные для входа, сбрасывают пароли и перепродают полученную информацию. Хотя игровая учетная запись кажется несильно значимой для безопасности, в ряде случаев она таковой является. Крайне важно, чтобы разработчики игр учитывали опасности онлайн-пиратства и инициативно боролись с ним, брали на себя ответственность в этой борьбе и активно проводили просветительскую работу, повышая цифровую гигиену.

Вовлечение детей в радикально-экстремистские, криминально ориентированные организации и неформальные объединения. Несовершеннолетние попадают в подобные круги из-за недостатка жизненного опыта или пребывания в трудной ситуации, когда соблазняются возможностью заработать. В сетевых сообществах с аморальной или противоправной деятельностью добиваются целенаправленного подчинения участников. Нередко такими процессами руководят опытные психологи, применяя отработанные годами методы влияния на детей.

Негативные примеры для подражания. В погоне за популярностью некоторые блогеры публикуют экстремальные видео, в которых подвергают себя риску, и не озвучивают последствий разного рода экспериментов. Уязвимые дети часто пробуют повторять их действия, иногда с катастрофическим или даже фатальным исходом. Дело в том, что такие ролики стирают границы между реальностью и фантазией, провоцируя несовершеннолетних на необдуманные поступки.

Пропаганда насилия. В Сети имеет место контент, который утверждает агрессию по отношению к другим в качестве нормы. Просматривая его, дети лишаются сострадания.

Потеря ценностей. Систематичное поглощение токсичных материалов приводит несовершеннолетних к потере чувствительности. Спустя некоторое время неадекватный контент воспринимается детьми как обычное явление, не вызывает негативной реакции.

В исследовании Национального центра пропавших без вести и эксплуатируемых детей США отмечается, что несовершеннолетние — одни из самых уязвимых членов общества. Правонарушители используют в отношении них следующие методы:

— вовлекают в сексуализированный диалог или ролевую игру с целью дальнейшего изнасилования или эксплуатации (34 %);

— просят показать фотографии сексуального характера (33 %);

— втираются в доверие через комплименты, обсуждение «общих» интересов, проявление заботы и сопереживания, позитивные лайки и комментарии (29 %);

— под ссылкой на интересный контент отправляют сексуализированные изображения (23 %);

— притворяются сверстниками или младшими по возрасту (20 %);

— предлагают отправить свои откровенные изображения (10 %);

— инициируют обмен сексуализированными фото (9 %), иногда даже в качестве компромисса в общении;

— обещают заманчивое вознаграждение в обмен на достижение цели: деньги, подарочную карту, желаемые товары и услуги, сигареты, алкоголь, наркотики, предоставление жилья, транспорта, питания (8 %);

— Более редко (<5 %) злоумышленники делают следующее: выдают себя за женщину, модельного агента, фотографа или знакомого, используя фальшивый или украденный аккаунт;

— делают скрины или сохраняют детские фото, видео и записи без разрешения;

— используют для общения автоматизированные системы.

Родителям при создании безопасной цифровой среды для детей важно знать о возможных онлайн-рисках. Существует ряд опасностей, связанных с использованием определенных сайтов и мобильных приложений. Можно выделить ряд моментов, на которые следует обратить внимание при оценке безопасности интернет-ресурса для ребенка:

— наличие неверного, пагубного, оскорбительного контента;

— наличие материалов для взрослых;

— присутствие на ресурсе пользователей всех возрастов;

— наличие не отслеживаемых администратором чатов, групп и форумов;

— наличие непрозрачных и сложных для понимания элементов управления конфиденциальностью;

— использование видеотрансляций в режиме реального времени;

— возможность применения геометок о местоположении пользователей. наличие функции звонков, которые не отображаются в журнале вызовов устройства; высокий уровень анонимности на ресурсе.

На ресурсе SafeWise указаны следующие опасные для детей приложения:

— социальные сети YouTube, Snapchat, TikTok, Instagram, Tumblr, Reddit, Facebook, Twitter, Qzone, Tout, Spreely, Triller, MeWe, Gab, Rumble, Social, IRL, YikYak, Hoop, GETTR, VSCO, WeChat, Wishbone, Marco Polo;

— приложения для потокового вещания LiveMe, Houseparty, Big Live, BIGO Live, Uplive, Clover, REALITY, Quibi, Twitch, Tango, Yubo, Livestream, Nonolive, YouNow, Spoon, 17LIVE, SuperLive, MICO, Imo live, Hakuna, Likee, Coco, Ly, Camsurf, Omega, Hola, Marco Polo;

— чаты WhatsApp, Messenger, Line, Discord, Kik, Viber, Telegram, Caffeine, Clubhouse, IMVU, Friends, Fam, Threema, Wink, Itsme, BOSS Revolution, Chatjoy, Imo, Nowchat, Signal, Hangouts, Addchat, Wizz, BOTIM, BiP, Anonymous Chat Room, Cheers, Squad, Byte, Omegle, Tellonym;

— многопользовательские игры со встроенными чатами Drug Grand Mafia, Zepeto, Among Us, Modern Combat, PUBG, LifeAfter, The Wolf, Call of Duty, «Tom and Jerry: The Chase», «Suspects: Mystery Mansion», Super Mecha Champions, Spaceteam, Hago, Rules of Survival, Slam Dunk;

— приложения для знакомств Tinder, Grindr, Plenty of Fish, Hily, Match, Zoosk, Mocospace, MeetMe, Bumble, BLK, Skout, Badoo, Hot or Not, Tagged, Upward, Luxy Celebs, Ashley Madison, SweetRing, Flirtini, Cougar, CougarD, Taimi, 3Fun, Bustr, Geek Seek, Clover, Chispa, Flourish, Popcorn, Hinge, Ayala, Kinkoo, AChat, Hookup, Pure, XDate, 3rder, Gaper, Adult Chat, Hook Me Up, KS, Wild, Cuff, FWB, Shake It, Pernals, Feeld, Flirt Me, InMessage, EZMatch, Surge, Military, Ace, Chaturbate, 3somer, Juicy;

— ресурсы с порнографией iGirl, Dipsea, Juice Live, Lifestyle for Men, Kegel, JoyHouse, Naughty Video Chat, Tickle Her, Galatea, Radish Fiction;

— сюжетные игры или симуляторы Scandal, Kiss Kiss, «Stories: Your Choice», My Fantasy, Producer, Campus, Dream Zone, Hotel Hideaway, Chapters, Ikemen Vampire, Episode, BloodKiss, The Arcana;

— дипфейк-разработки Reface, FaceMagic, Avatarify, iFace, Wombo, FakeMe, Impressions, MyHeritage, DeepFaceLab, FaceApp, FaceSwap, FacePlay, Jiggy, iFake;

— приложения для майнинга Bitcoin 2021, Bitcoin (BTC), Crypto Holic, MineBit Pro, BitFunds, Daily Bitcoin Rewards, Ethereum;

— секретные хранилища данных Best Secret Folder, Calculator, Privault, Secret;

— анонимные приложения FM, Whisper, Lipsi, Tellonym.

К другим проблемным разработкам SafeWise отнес Google Doc и приложения о сдаче недвижимости.

Также в приложении № 2 данного обзора представлен список ресурсов, популярных среди детей, с которыми необходимо ознакомиться родителям.

СТАТИСТИКА И ПОКАЗАТЕЛИ ПО РАССМАТРИВАЕМОЙ ПРОБЛЕМЕ

Согласно данным UNICEF, каждый третий интернет-потребитель — ребенок до 18 лет. При этом сексуальная эксплуатация — одно из наиболее прибыльных преступлений в мире. По подсчетам некоммерческой организации Enough is Enough, ей подвергаются до 5 % детей Земли. Наряду с этим в последнее десятилетие число подобных преступлений во всем мире только растет. По информации некоммерческой организации по безопасности детей Internet Watch Foundation, в 2021 году более 250 тысяч URL-адресов содержали изображения сексуального насилия над детьми. Это на 64 % больше, чем в 2020-м.

Интересен и другой факт. Недавнее исследование инновационной платформы UNICEF «U-Report» показало: локдаун, введенный из-за пандемии COVID-19, обнажил неравенство доступа к цифровому обучению среди людей от 18 до 35 лет:

— Только 11% молодежи имеют ноутбук с выходом в Сеть.

— 41% молодых людей пользуются личным смартфоном, но лишь 17% — с интернет-пакетом.

— При этом 41% респондентов нуждаются в обучении цифровым навыкам.

В разделе о статистике важно также упомянуть о существовании Индекса детской безопасности в Интернете (The Child Online Safety Index, COSI). Он измеряет в режиме реального времени уровень онлайн-защищенности несовершеннолетних во всем мире.

Это делается на основе анализа шести областей:

— киберрисков;

— дисциплинированного использования цифровых технологий;

— цифровой компетентности;

— поддержки детей взрослыми и качества организации образовательного процесса;

— социальной инфраструктуры;

— возможностей подключения.

Каждая из областей состоит из двух-восьми целевых индикаторов. Это позволяет проводить всестороннюю оценку онлайн-безопасности детей. Для каждой страны рассчитывается показатель COSI в диапазоне от 0 (самый низкий) до 100 (самый высокий).

Возвращаясь к кибербуллингу, следует отметить исследования ресурса SafeWise о том, что более 36 % детей от 12 до 17 лет подвергались ему в определенный момент жизни и почти 15 % — издевались над кем-то в Интернете. При этом потерпевшими онлайн-хищников становились несовершеннолетние от года до 17 лет. Когда дело доходило до онлайн-соблазнения, девочки составляли большинство детей-жертв (78 %), в то время как большая часть онлайн-хищников (82 %) была мужчинами. Интересен еще тот факт, что 98 % из них никогда не достигали своих целей в отношении детей в реальной жизни.

Почти половина респондентов бизнес-платформы Statista согласилась с тем, что в 2019 году наибольшей интернет-угрозой для российской молодежи была онлайн-вербовка в экстремистские группировки. На втором месте оказались виртуальные группы смерти, поощрявшие самоубийства подростков. А наиболее негативное влияние на российскую молодежь тогда же, по мнению 26

% участников опроса, оказал кибербуллинг.

Кроме того, в 2019 году более 90 % родителей детей до семи лет заявили, что проверяли действия чад в Интернете. Среди родителей подростков доля следящих за онлайн-жизнью детей была зафиксирована на уровне 61 %.

МИРОВАЯ ПРАКТИКА: ПОДХОДЫ СТРАН, МЕЖДУНАРОДНЫХ ОРГАНИЗАЦИЙ, ПРАВОЗАЩИТНИКОВ И ИССЛЕДОВАТЕЛЬСКИХ ПЛОЩАДОК К ВОПРОСАМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДЕТЕЙ В ИНТЕРНЕТЕ

ИССЛЕДОВАНИЯ, ПРОЕКТЫ, ИНИЦИАТИВЫ, КОНЦЕПЦИИ, ПРОГРАММЫ, ИНСТРУМЕНТЫ «МЯГКОГО ПРАВА» РАЗЛИЧНЫХ МЕЖДУНАРОДНЫХ ОРГАНИЗАЦИЙ И

ПЛОЩАДОК

Перед рассмотрением инициатив следует отметить, что права детей изложены в ряде международных и региональных документов по правам человека, в том числе в:

— Всеобщей декларации прав человека от 10 декабря 1948 года, в статьях № 25 и № 26;

— Международном пакте ООН о гражданских и политических правах от 16 декабря 1966 года;

— Европейской конвенции о защите прав человека и основных свобод от 4 ноября 1950 года, в статье № 8;

— Конвенции Совета Европы о защите детей от сексуальной эксплуатации и сексуального насилия от 1 июля 2010 года;

— Хартии основных прав Европейского союза от 7 декабря 2000 года, в статье № 24;

— Международном пакте об экономических, социальных и культурных правах от 16 декабря 1966 года;

— Конвенции № 108 о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года и Протоколе «Конвенция № 108+»;

— Общем регламенте о защите персональных данных Европейского парламента и Совета Европейского союза от 27 апреля 2016 года;

— Руководстве Организации экономического сотрудничества и развития по защите неприкосновенности частной жизни и трансграничной передаче персональных данных 1980 года с изменениями 2013-го;

— Конвенции ООН о правах ребенка от 20 ноября 1989 года;

— Замечании общего порядка № 25 ООН о правах детей в связи с цифровой средой от 2 марта 2021 года;

— Европейской конвенции об осуществлении прав детей от 25 января 1996 года;

— Рекомендации Совета Организации экономического сотрудничества и развития о детях в цифровой среде от 31 мая 2021 года;

— Рекомендации CM/Rec7 Комитета министров Совета Европы государствам-членам о Руководстве по уважению, защите и реализации прав ребенка в цифровой среде от 4 июля 2018 года;

— Рекомендации CM/Rec10 Комитета министров Совета Европы государствам-членам о развитии обучения цифровой гражданственности от 21 ноября 2019 года;

— Руководстве Совета Европы по защите персональных данных детей в образовательной среде от 2020 года;

— Декларации Комитета министров Совета Европы о необходимости защиты частной жизни детей в цифровой среде от 28 апреля 2021 года;

— Резолюции о защите конфиденциальности в социальных сетях

— XXX Международной конференции уполномоченных по защите данных и конфиденциальности от 17 октября 2008 года;

— Резолюции о конфиденциальности детей в Интернете XXX Международной конференции уполномоченных по защите данных от 17 октября 2008 года;

— Рабочем документе Международной рабочей группы по защите данных в телекоммуникациях «Защита конфиденциальности детей в онлайн-сервисах» от 9–10 апреля 2019 года;

— Декларации о защите детей ото всех форм онлайн-эксплуатации и жестокого обращения Ассоциации государств Юго-Восточной Азии 2019 года.

ООН И УЧРЕЖДЕНИЯ СИСТЕМЫ ООН

Генеральная ассамблея ООН в 1989 году приняла Конвенцию ООН о правах ребенка. В ней закреплены права граждан, не достигших 18 лет. Согласно документу, все дети имеют право на уважительное обращение, защиту, развитие потенциала и участие в общественной жизни. 196 государств обязались оберегать несовершеннолетних от насилия, в том числе от сексуальных надругательств и эксплуатации в Интернете. Текст конвенции также указывает на важность диалогов с детьми об их правах на защиту данных.

Резолюция «Право на неприкосновенность частной жизни в цифровой век» Генеральной ассамблеи и Совета по правам человека ООН от сентября 2019 года отмечает, что люди, в том числе и дети, должны быть обеспечены в Интернете такими же правами, что и в реальной жизни.

Стратегия ООН «Молодежь-2030» ставит своими целями укрепление потенциала и расширение прав молодых людей по всему миру посредством наращивания региональных, страновых и глобальных усилий в этой сфере. Кроме того, политикой документа предусмотрено участие молодежи в реализации Повестки дня ООН на период до 2030 года.

В рамках стратегии также составлен систематизированный онлайн-сборник моделей работы с молодыми людьми. Собрание, созданное при участии молодежи, представляет собой инструментарий из более чем 750 практических советов по основополагающим областям стратегии.

МЕЖВЕДОМСТВЕННАЯ РАБОЧАЯ ГРУППА ООН ПО ВОПРОСУ О НАСИЛИИ В ОТНОШЕНИИ ДЕТЕЙ (UNIAWG-VAC)

Повестка Межведомственной рабочей группы ООН по вопросу о насилии в отношении детей (The UN Inter-Agency Working Group on Violence against Children, UNIAWG-VAC) указывает на необходимость обучения несовершеннолетних ответственному поведению в Интернете и развития у них цифровых навыков. Из конкретных действий повестка рекомендует проверять пользовательский контент и информировать о вредоносном содержании, разжигании ненависти и другом незаконном поведении. Также в документе даются советы родителям о лучших способах онлайн и офлайн-защиты детей, в том числе о том, как реагировать на обнаружение вредного контента и небезопасных контактов и куда при необходимости сообщать об этом.

Кроме того, в упомянутом документе образовательным учреждениям рекомендуется обновить политику безопасности, отразив в ней риски онлайн-обучения. Частному сектору рекомендовано прибегнуть к фильтрации и модерации контента, а также к инструментам родительского контроля: проверка возраста пользователей для предоставления им только подходящей информации; защита контента паролем; сверка со списками ресурсов, подлежащих блокировке; отслеживание покупок; мониторинг проведенного в Сети времени.

Детский фонд ООН (UNICEF) Страновые и региональные отделения Детского фонда ООН (United Nations Children's Fund, UNISEF) реализуют порядка 40 инициатив. Часть из них направлена на развитие компетенций и навыков в цифровой среде, другие — на безопасность в Интернете.

Согласно мнению UNISEF, обязанность защищать детей в цифровом мире лежит на всех, включая правительства, семьи и школы. Однако бизнес, особенно в технологической и телекоммуникационной отраслях, несет повышенную ответственность за воздействие цифровых технологий на несовершеннолетних. Частный сектор должен продвигать общеотраслевые этические стандарты в отношении данных и конфиденциальности, а также других видов практик по защите детей в Интернете.

Сегодня UNISEF реализует важный проект — «Безопасные чат-боты». Для начала стоит отметить, что чат-бот — это один из новейших цифровых продуктов, который с помощью виртуального собеседника выявляет потребности пользователей, а после удовлетворяет их. UNISEF в Руководстве о внедрении безопасных чат-ботов предлагает решения по улучшению мер защиты таких онлайн-разработок.

По данным UNISEF, все больше и больше людей, включая детей, используют автоматизированных советчиков для получения информации. При правильном исполнении, а именно включении искусственного интеллекта для интерпретации сообщений пользователей, чат-боты предлагают персонализированное консультирование. Однако, как и любая новая технология, они также создают и беспрецедентные проблемы в области безопасности, так как чаще всего все-таки представляют собой заранее выстроенные «деревья решений».

Дело в том, что порой чат-боты получают жизненно важные сообщения. Несовершеннолетние, находящиеся в трудном положении или получившие травматический опыт, рассматривают

автоматизированных собеседников как способ обратиться за помощью. Но проблема в том, что, как было оговорено ранее, многие чат-боты не настроены для оказания такого рода услуг. Поэтому нуждающиеся в помощи вместо нее получают ненужную или недостоверную информацию или, что еще хуже, автоматический ответ, который только усугубляет подавленность пользователя, нанося ему еще больше вреда.

Ввиду всего вышесказанного также стоит отметить, что шаги по улучшению чат-ботов с точки зрения просвещения и поддержки несовершеннолетних в области сексуальных проблем представлены в бюллетене UNISEF «Защита девочек и мальчиков».

Также стоит обратить внимание на аналитическую записку UNISEF «Цифровое обучение для каждого ребенка: устранение пробелов для инклюзивного и процветающего будущего» от сентября 2021 года, в которой даются следующие рекомендации:

— Оказывать психологическую помощь и разрабатывать предложения для детей и родителей, чтобы помочь им справиться с переходом на цифровое обучение во время таких кризисов, как COVID-19. Советы должны включать способы поддержания здорового сна и временного баланса между личной, общественной жизнью, образовательным процессом и досугом, так как некоторые дети сообщали о цифровой усталости из-за увеличения времени, которое они проводят в онлайне.

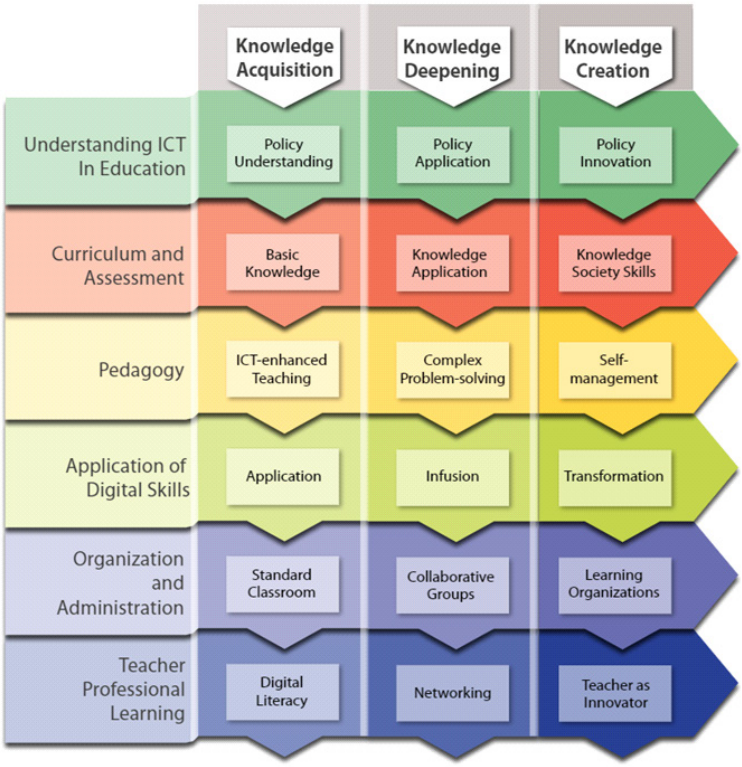
— Обеспечивать безопасность несовершеннолетних в Интернете, встраивая средства защиты в продукты для цифрового обучения. Ведь по мере увеличения времени нахождения в Сети уязвимые дети больше подвергаются онлайн-рискам и становятся менее способными найти поддержку.

— Внедрять инновационные стратегии предотвращения насилия над несовершеннолетними и их эксплуатации, а также стратегии быстрого реагирования на подобные инциденты.

По мнению Европейской комиссии, высказанном в документе «Стратегия по наиболее эффективной борьбе с сексуальным насилием над детьми» от июля 2020 года, такие инструменты нужно ориентировать на возраст и пол ребенка, строить на основе фактов, полученных от детей, а также учитывать национальный и местный контексты.

При этом эксперты в тематике исследования в соцсети ResearchGate высказывают мнение

Рисунок № 2



Источник: UNESCO, «Структура ИКТ-компетентности учителей»

о том, что эти системы предотвращения и реагирования нужно интегрировать в национальную политику защиты несовершеннолетних.

УЧРЕЖДЕНИЕ ООН ПО ВОПРОСАМ ОБРАЗОВАНИЯ, НАУКИ И КУЛЬТУРЫ (UNESCO)

В 2015 году в Париже 184 государства из Учреждения ООН по вопросам образования, науки и культуры (United Nations Educational, Scientific and Cultural Organization, UNESCO) утвердили Рамочную программу действий «Образование-2030». Документ призван обеспечить всех людей справедливым качественным образованием, которое можно получить на протяжении всей жизни.

В 2019 году UNESCO разработала рекомендации «Структура ИКТ-компетентности учителей». В них даются советы по организации обучения преподавателей использованию информационно-коммуникационных технологий (ИКТ) и говорится о важности приобретения педагогами цифровых навыков для повышения качества образования.

Согласно документу, на уровне получения знаний учитель должен использовать текстовые редакторы, почтовые программы и программы для создания презентаций, а также ресурсы социальных сетей. На уровне освоения знаний педагогу необходимо уметь самостоятельно определять, какие инструменты лучше подойдут для решения разного рода задач. А на уровне создания знаний преподаватель должен самостоятельно внедрять инновации в процесс обучения.

В перечисленных выше уровнях знаний UNESCO выделяет шесть основных аспектов, отражающих стандартные обязанности учителей (рисунок № 2):

— роль ИКТ в образовательной политике;

— учебная программа и оценивание;

— педагогические практики;

— цифровые навыки;

— организация образовательного процесса и управление им;

— профессиональное развитие педагогов.

Также стоит отметить, что «Структура ИКТ-компетентности учителей» основана на принципах всеобъемлющего обучения и отсутствия дискриминации, свободного и равного доступа к информации в сфере образования с использованием современных технологий. Кроме того, в документе рассказывается о том, как последние технологические достижения — искусственный интеллект, «Интернет вещей» и другие — способствуют формированию инклюзивных обществ знаний.

Отмечается, что основа успешного применения рекомендаций зависит от последовательной поддержки государств — постоянных инвестиций в обучение педагогов. Именно поэтому в документе также представлены советы о том, как содействовать повышению квалификации преподавателей в различных условиях.

КОМИТЕТ ООН ПО ПРАВАМ РЕБЕНКА

В Пояснительных замечаниях общего порядка № 25 от 2021 года Комитета ООН по правам ребенка отмечается, что во всех законодательных актах необходимо уделять внимание защите прав детей и выявлению рисков для них, то есть принимать меры еще до причинения вреда несовершеннолетним. Поэтому обновление законодательств должно стать политическим приоритетом.

Кроме того, по мнению Комитета ООН по правам ребенка, государства должны финансово поддерживать соответствующие регулирующие и правоохранительные органы, гарантировать их юридические полномочия и технические знания. В документе также звучит призыв к сотрудничеству между бизнесом, правительствами, гражданским обществом, учреждениями ООН и другими международными организациями для постановки детей в центр цифровой политики. Согласно пояснительным замечаниям, такой результат должен быть достигнут осуществлением нескольких мер, среди которых:

— Координация глобальных, национальных и региональных мероприятий. Политики, правоохранители и технологическая индустрия должны углубить сотрудничество для внедрения принципов безопасности в инновации, чтобы предотвратить сексуальные надругательства над детьми и их эксплуатацию в Интернете.

— Защита конфиденциальности несовершеннолетних. Для ее реализации следует применять международные стандарты при сборе и использовании данных о детях в Сети.

— Расширение прав и возможностей детской аудитории в Интернете посредством ее обучения цифровой грамотности. Правительства и технологи должны плотно взаимодействовать при разработке образовательных платформ и учебных программ от начальной до средней школы. Также властям

нужно поддерживать расширение возможностей онлайн- и публичных библиотек по обучению цифровым навыкам и инвестировать в цифровую грамотность учителей.

— Использование уникальной роли частного сектора. Бизнес должен обеспечить соблюдение общеотраслевых этических стандартов в отношении данных и конфиденциальности детей в Интернете. При этом эти стандарты должны касаться как разработки продуктов, так и маркетинга.

— Инвестирование в получение более качественных фактических данных о возможностях несовершеннолетних в Сети и онлайн-опасностях для них. Впоследствии собранную информацию необходимо использовать для создания нормативно-правовой базы и практик, признающих особые потребности детей.

МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ (ITU)

Международный союз электросвязи (International Telecommunication Union, ITU) реализует Руководство по защите детей в онлайн-среде от мая 2021 года на политическом и оперативном уровнях. Молодежная повестка ITU сосредоточена на содействии развитию цифровых навыков и создании возможностей трудоустройства молодежи посредством ИКТ-инструментов.

Согласно данным ITU, сегодня в мире Интернетом пользуются 71 % молодых людей. Тогда как в других возрастных группах ко Всемирной сети обращаются 57 % населения планеты. Из этого следует, что офлайн- и онлайн-будни молодежи неразрывно связаны и в равной степени влияют на ее благополучие и перспективы.

Необходимость защиты детей от эксплуатации и других опасностей при использовании Интернета была отмечена ITU еще в 2015 году — в Заключительных актах Полномочной конференции. На самом мероприятии в 2014-м прозвучал призыв к принятию на международном уровне упреждающих мер для безопасности несовершеннолетних в онлайн-среде.

В 2010 году состоялось первое заседание Рабочей группы Совета ITU по защите детей в Интернете — единой платформы союза, на которой государства-члены, участники сектора и внешние эксперты обмениваются мнениями и продвигают тематическую деятельность. На этой площадке были созданы практические рекомендации по безопасности в Сети для разных групп мирового населения — детей и родителей, политиков и деятелей промышленности.

Говоря о деятельности ITU по теме исследования, следует отметить Комиссию по широкополосной связи, созданную союзом совместно с UNESCO. Одна из ее центральных целей — распространять информацию о значимости широкополосной связи на различных международных собраниях и привлекать высокопоставленных лиц к развитию ее инфраструктуры и услуг во всем мире.

Комиссия сыграла важную роль в запуске ряда глобальных решений в сфере безопасности несовершеннолетних в Интернете. Среди них — инициатива «Защита детей в онлайн-среде», направленная на повышение информированности общества и разработку инструментов для снижения рисков. В ее рамках, в ключе Глобальной программы кибербезопасности ITU, в 2020 году были разработаны Руководящие принципы по защите несовершеннолетних в онлайн-среде для директивных органов по всему миру. Их целью стало создание основ безопасной цифровой среды не только для сегодняшних детей, но и для будущих поколений, в том числе для представителей уязвимых групп — детей-мигрантов, детей с расстройством аутистического спектра и ограниченными возможностями.

Кроме того, ITU участвует в глобальной инициативе «Достойные рабочие места для молодежи» и возглавляет совместно с Международной организацией труда кампанию «Цифровые навыки для рабочих мест».

Также ITU совместно с Одесской национальной академией связи имени А. С. Попова в рамках реализации второй Региональной инициативы для стран СНГ разработал Мультимедийный учебный дистанционный курс безопасного пользования ресурсами Интернета. Он включил в себя базовый, средний и продвинутый уровни.

Базовый уровень рассчитан на детей дошкольного и младшего школьного возрастов. Его задача — донести до ребенка общие сведения о безопасности в Интернете. А помогает в этом виртуальный помощник в виде мальчика или девочки, который периодически еще и задает вопросы для закрепления полученных знаний. После прохождения уровня ребенок, к примеру, сможет различать полезные и вредоносные виртуальные игры. Сертификат о завершении обучения выдается в конце автоматически.

Средний уровень создан для учеников 5–9 классов. Он нацелен не только на информирование

об онлайн-рисках, но и на формирование стойкой мотивации для соблюдения правил безопасности в Сети. В его рамках также предусмотрено развитие критического мышления на примере оценки достоверности сведений из Интернета, просмотр пяти мультипликационных роликов и прохождение двух интерактивных игр.

По завершении обучения ребенок решает тест из десяти вопросов и в случае правильных ответов получает сертификат.

Продвинутый уровень ориентирован на старшеклассников, студентов, родителей и педагогов. Обучающиеся не только узнают о типичных сценариях онлайн-мошенников и конкретных правилах безопасного использования Сети, но и смогут самостоятельно идентифицировать онлайн-риски. На этом уровне также дается информация о конфиденциальности и работе через публичные сети, обсуждается поведение в сложных ситуациях, а также описываются методы фильтрации контента и защиты детей в Интернете. По завершении каждого модуля проводится тестирование. В конечном итоге при успешной сдаче всех экзаменов генерируется сертификат о прохождении обучения.

Кроме того, на платформе содержится автоматическая рекомендательная система, которая предназначена для подбора каждому пользователю оптимальных мер фильтрации контента в Интернете. Сначала программное обеспечение определяет уровень квалификации абонента — от новичка до эксперта — при помощи небольшого теста по компьютерной грамотности. Затем при ответе пользователя на несколько вопросов формулируются его основные требования к методам фильтрации, после чего система выдает конечные рекомендации для конкретного случая.

Кроме всего прочего, ITU разработал Всеобщую декларацию безопасности детей в Интернете. Она направлена на объединение всех заинтересованных сторон в общем деле обучения несовершеннолетних с разным жизненным опытом цифровым навыкам для их перспективного будущего.

Еще один документ ITU, о котором необходимо упомянуть в рамках исследования, — отчет «Статистическая основа и показатели онлайн-безопасности детей» 2010 года.

В нем представлен список параметров для международных сопоставлений и даны рекомендации по сбору данных. Благодаря этому документу государства-члены смогут оценить степень защищенности детей в онлайн-среде и определить аспекты, которые требуют дополнительных усилий.

ФОРУМ ПО УПРАВЛЕНИЮ ИНТЕРНЕТОМ (IGF)

Форум по управлению Интернетом (Internet Governance Forum, IGF) ежегодно предоставляет международную площадку для обмена мнениями по актуальным вопросам развития Сети. В частности, темы цифровой безопасности несовершеннолетних обсуждает Динамическая коалиция IGF по защите детей в онлайн-среде. В ее программу в 2016–2018 годах включались следующие вопросы:

— обеспечить наиболее безопасную онлайн-среду для детей;

— наладить регулярный обмен опытом между заинтересованными сторонами;

— поощрить совершенствование правовых норм и инструментов саморегулирования в целях обеспечения защиты детей в Интернете;

— активизировать на всех уровнях усилия по борьбе с сексуальным надругательством над несовершеннолетними;

— стимулировать расширение прав и возможностей детей;

— обсудить вопрос об обеспечении разумного использования инструментов, ограничивающих доступ несовершеннолетних к определенным типам контента и услуг; добиться учета потребностей детей при разработке новых онлайн-услуг и приложений;

— создать диалоговую платформу для агентств по правам ребенка и защитников свободы выражения мнений.

В ноябре 2020 года IGF провел круглый стол «Определение прав детей в повестке дня управления Интернетом: баланс рисков и возможностей». Во время него поднимались вопросы паритета доступа несовершеннолетних к информации и их защиты от насилия, разжигания ненависти, сексуальных надругательств и эксплуатации в онлайн-среде. Кроме того, обсуждалось повышение устойчивости детей к угрозам в Интернете путем наращивания потенциала их навыков и знаний, поддержки и руководства в цифровой среде, а также совершенствования многосторонних механизмов сотрудничества.

В декабре 2021 года дискуссия IGF формировалась вокруг проблем и возможностей регулирования цифровой сре-

ды. При этом приоритетной задачей на 2022-й IGF считает обсуждение вопроса о целесообразности смещения акцента в работе с защиты детей в онлайн-среде на непосредственное участие несовершеннолетних в этой самой защите. Кроме того, еще одной важной целью на ближайшее будущее IGF называет стремление к сотрудничеству с другими объединениями для решения многих проблемных моментов, среди которых:

— кибербезопасность детей;

— цифровые интеграция и развитие с ориентиром на права несовершеннолетних;

— учет детской безопасности при разработке цифровых сервисов;

— шифрование;

АНАЛИЗ ОСНОВНЫХ ЦЕННОСТЕЙ ИНТЕРНЕТА. МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ТРУДА (ILO)

Международная организация труда (The International Labour Organization, ILO) проводит кампанию по развитию цифровых навыков в целях создания достойных рабочих мест для молодежи. Ее цель — стимулировать заинтересованных лиц обучать молодых людей с возможностью дальнейшего трудоустройства в условиях цифровой экономики.

Также ILO уделяет внимание и отдельным вопросам онлайн-защиты детей, в частности связанным с принудительным трудом, современным рабством и торговлей людьми в различных странах мира.

ОРГАНИЗАЦИЯ ЭКОНОМИЧЕСКОГО СОТРУДНИЧЕСТВА И РАЗВИТИЯ (OECD)

Вопросы защиты детей в Интернете включены в повестку основных рабочих органов по образованию, инновациям, здравоохранению, труду и занятости Организации экономического сотрудничества и развития (Organization for Economic Cooperation and Development, OECD). По ряду направлений OECD является основоположником в разработке международных документов рекомендательного характера по данной тематике.

Основная деятельность OECD в сфере защиты несовершеннолетних в онлайн-среде ведется на площадке Комитета по политике в области цифровой экономики и включает разработку статистических рамок и практических руководств. Проекты OECD имеют комплексный, горизонтальный характер.

OECD признает, что Интернет стал повседневной реальностью в жизни несовершеннолетних, привнес как значительные выгоды для их образования и развития, так и подверг их онлайн-рискам. Такая ситуация создала необходимость оказания поддержки правительствам и другим заинтересованным сторонам в создании безопасных, полезных и справедливых условий для всех детей в цифровой среде.

В связи с потребностями онлайн-сообщества в феврале 2012 года OECD разработала Рекомендацию о защите детей в цифровой среде и с учетом меняющихся реалий обновила ее в мае 2021-го. В документе даются четкие инструкции по совершенствованию правовых и политических мер реагирования в соответствии с технологическим прогрессом, а также по разработке прочной доказательной базы и ответных на онлайн-преступления действий.

В числе политических мер указываются:

— законодательные мероприятия, а также прямые и косвенные инструменты политики;

— участие в политической разработке заинтересованных сторон;

— инициативы по трансграничному сотрудничеству и обмену знаниями.

Кроме того, в целях многостороннего диалога заинтересованных сторон в апреле 2021 года OECD приняла дополнение к Рекомендации о защите детей в цифровой среде — Руководство для поставщиков цифровых услуг. В нем организация перечислила конкретные действия, к которым должны прибегать интернет-разработчики во избежание нарушения прав и безопасности несовершеннолетних при проектировании, разработке, внедрении и эксплуатации продуктов. Для этого поставщикам цифровых услуг необходимо:

— предотвращать доступ несовершеннолетних к контенту, который не соответствует их возрасту, может нанести ущерб здоровью и благополучию или ущемить их права;

— продолжать анализировать эффективность защитных мер и при необходимости улучшать их;

— регулярно тестировать изменения в технологиях на предмет появления новых онлайн-рисков для детей.

При этом OECD подчеркивает, что, хотя поставщики цифровых услуг и призваны соблюдать ее рекомендации, конкретные принимаемые ими действия могут значительно отличаться от модельных мер из-за разницы в национальных правовых и нормативных контекстах, а также в профилях опасностей предоставляемых продуктов. В данном случае эксперты советуют делать акцент на принятии мер пропорционально рискам.

Стоит отметить, что в фокусе OECD также находится вопрос детского благополучия в период пандемии COVID-19. Во время локдауна цифровая среда все больше становилась ареной как для образовательных, так и для социальных детских мероприятий и несовершеннолетние проводили все больше времени в ней. В связи с этим росли объемы собираемой информации о детях, а следовательно, росла и степень потенциальных онлайн-угроз для них.

В качестве ответа на сложившуюся ситуацию в июне 2020 года OECD опубликовала обзор последних изменений в нормативно-правовой базе и политике «Защита детей в Интернете». В нем был выделен ряд требующих предметного законодательного рассмотрения мер, среди которых оказались:

— уделение должного внимания обеспечению безопасной и полезной цифровой среды для детей, в том числе за счет конструктивного подхода к устранению рисков;

— предоставление несовершеннолетним и их родителям информации о сборе, раскрытии и передаче третьим лицам их персональных данных;

— гарантия мер предосторожности в отношении конфиденциальности материалов о детях, в том числе их защита от коммерческого использования;

— демонстрация соблюдения внутренних политик, нормативных актов или законов по онлайн-безопасности несовершеннолетних.

Также важным этапом работы OECD по онлайн-защите детей стало создание в 2017 году Информационного портала о благополучии несовершеннолетних. На нем представлено 52 межнациональных показателя по различным областям тематики — домашней среде, состоянию здоровья, качеству образования, внешкольным мероприятиям, удовлетворенности жизнью и информации о государственной политике. При этом материалы адаптированы для разных пользователей, в зависимости от возраста, пола, семейного дохода, уровня образования и миграционного статуса семьи.

В июле 2021 года OECD опубликовала документ «Измерение показателей благополучия детей», который также включил в себя индекс действий несовершеннолетних в онлайн-среде. В тексте, к примеру, к ключевым аспектам благополучной жизни детей был отнесен доступ к цифровым инструментам — компьютерам, планшетам, видеоиграм, Интернету.

Другим фактором, влияющим на счастливую жизнь несовершеннолетних, OECD определяет эмоциональное благополучие. Подробнее Центр образовательных исследований и инноваций OECD рассмотрел его в книге «Воспитание детей XXI века: эмоциональное благополучие в эпоху цифровых технологий» от октября 2019 года.

Так, по мнению экспертов издания, решающее значение для современных несовершеннолетних имеет воспитательный подход «единство в многообразии». Кроме того, важно развивать у детей когнитивные навыки, цифровую грамотность и способность саморегулироваться в процессе обучения.

МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ УГОЛОВНОЙ ПОЛИЦИИ (INTERPOL)

Международная организация уголовной полиции (International Criminal Police Organization, Interpol) реализует ряд проектов для поддержки стран в борьбе с сексуальной эксплуатацией детей и онлайн-насилием над ними с использованием цифровых, интернет- и коммуникационных технологий. Такого рода преступления могут происходить онлайн или посредством сочетания онлайн-и личных взаимодействий между правонарушителями и детьми.

Количество материалов на тему сексуального надругательства над несовершеннолетними значительно увеличилось во время пандемии коронавируса. Об этом свидетельствует отчет Interpol «Влияние COVID-19 на сексуальное насилие над детьми» от сентября 2020 года.

Чтобы обеспечить безопасность детей в Сети, Interpol подготовил рекомендации для несовершеннолетних. Исходя из документа, детской аудитории следует:

— держать под контролем устройства: не раскрывать пароли, имена, номера телефонов, адреса проживания и другого местонахождения и регулярно проверять наличие высокой степени защиты в настройках конфиденциальности;

— не соглашаться на встречи с виртуальными друзьями в реальной жизни, предварительно не обсудив это со взрослыми;

— видеться с онлайн-товарищами, одобренными родителями, принимая меры предосторожности: сообщать близким о месте встречи или брать кого-нибудь с собой;

— дважды обдумывать намерение опубликовать или даже отправить в личные сообщения друзьям материалы неоднозначного характера;

— отказываться от участия в диалоге, если онлайн-взаимодействие чем-то не устраивает;

— делать снимки экрана для сохранения на устройстве беспокоящего контента;

— сообщать без смущения взрослым, если было совершено или опубликовано что-то, о чем стоит сожалеть.

Родителям Interpol для онлайн-защиты детей рекомендует вести открытый и честный диалог об использовании ресурсов Сети, поощрять безопасные привычки, говорить о различиях хорошего и плохого контента и осведомлять о киберугрозах.

Также стоит отметить, что в Interpol существует специальное подразделение по преступлениям против детей. В числе прочего оно занимается анализом фото- и видеоизображений в Интернете и на изъятых устройствах.

Есть еще несколько документов Interpol, важных для раскрытия темы. Среди них — Резолюция № 9 и Резолюция № 2 от ноября 2021 года, а также исследовательский проект «Разрушительный вред» от 2019-го, работа над которым велась в сотрудничестве с UNICEF и неправительственной некоммерческой общественной организацией по борьбе с сексуальной эксплуатацией детей ECPAT.

Резолюция № 9 поднимает проблемы расследования случаев сексуальной эксплуатации детей в Интернете и онлайн-насилия над ними. Среди них наиболее остро звучит использование в цифровой среде сквозного шифрования — метода, посредством которого только участники виртуального общения имеют доступ к диалогам. Именно он часто и становится загвоздкой в раскрытии онлайн-преступлений против несовершеннолетних. В связи с этим резолюция призывает поставщиков онлайн-услуг взять на себя ответственность за разработку безопасных для детской аудитории продуктов, в том числе без прибегания к сквозному шифрованию.

Резолюция № 2 направлена на улучшение процедуры международного взаимодействия, в частности процедуры обмена информацией о лицах, совершивших сексуальные онлайн-преступления против детей, с помощью уведомлений с зеленым углом, то есть уведомлений о злоумышленниках, проходящих по делу оперативного учета, но в отношении которых пока отсутствует процессуальное решение о признании подозреваемыми.

Исследовательский проект «Разрушительный вред», финансируемый Глобальным партнерством по ликвидации насилия в отношении несовершеннолетних, занимается разработкой практических решений для защиты детей от сексуального надругательства и эксплуатации как в Интернете, так и вне Сети. Его цель — разобраться в способах пособничества цифровых технологий совершению такого рода преступлений в 13 странах Восточной и Южной Африки. В рамках проекта уже подготовлены отчеты Кении, Уганды, Таиланда, Танзании, Филиппин и Эфиопии. Так, например, проект помог выявить, что на Филиппинах сексуальному надругательству и эксплуатации в Сети подвергаются два миллиона детей в год.

СОВЕТ ЕВРОПЫ (COE)

Согласно Рекомендации № 12 Комитета министров Совета Европы (Council of Europe, CoE) о расширении прав и возможностей детей в новой информационно-коммуникационной среде от сентября 2006 года, государства-члены должны применять многосторонний подход в решении поставленного вопроса. Документ также призывает поощрять деятельность бизнеса по развитию инициатив в области цифрового благополучия несовершеннолетних, в частности их информационной грамотности. Кроме того, коммерческим организациям предписывается внедрить систему внутренней оценки информационной политики и правила работы в цифровом пространстве в контексте безопасности несовершеннолетних и ответственного использования ими цифровой среды.

Также рекомендация побуждает поощрять гражданских субъектов, которые продвигают правозащитный аспект информационного общества, занимаются активным мониторингом, оценкой и поддержкой инициатив в области цифрового благополучия несовершеннолетних. Заключительное наставление документа — уделять повышенное внима-

ние роли детей и их наставников в новой информационно-коммуникационной среде.

Декларация Комитета министров CoE о защите достоинства, безопасности и частной жизни детей в Интернете от февраля 2008 года делает акцент на том, что только в рамках правоохранительной деятельности можно записывать контент, опубликованный несовершеннолетними в Сети, и только в том случае, если он угрожает их безопасности. Государствам-членам с привлечением других заинтересованных сторон предлагается изучить возможность сокрытия или удаления неправомерной информации, включая ее следы, в течение короткого периода времени.

Рекомендация № 5 Комитета министров CoE о мерах по онлайн-защите детей и содействию их активному участию в новой информационно-коммуникационной среде от июля 2009 года призывает государства-члены разработать совместную стратегию повышения информационной грамотности несовершеннолетних и их наставников.

В частности, обеспечить достаточное понимание детьми сути вопроса и наделить их соответствующими навыками. По мнению экспертов, информационная грамотность должна стать неотъемлемой частью всех этапов школьного образования. Полученные навыки научат несовершеннолетних правильно взаимодействовать с нежелательной информацией — о насилии, причинении вреда себе, дискриминации и тому подобном. Также такое обучение сформирует верную реакцию в случае издевательств, домогательств или преследований в цифровой среде.

Согласно документу, государствам-членам следует содействовать:

— разработке педагогических мер для обучения преподавателей распознаванию ситуаций, несущих риск, и ответственной реакции на них;

— реализации стратегии подготовки педагогов в условиях современной цифровой среды для расширения возможностей детей, находящихся на их попечении;

— проведению исследований поведения несовершеннолетних на разных этапах развития с привлечением бизнеса из цифровой отрасли.

Также в решении вопросов онлайн-безопасности детей в Сети имеют место Резолюция Парламентской ассамблеи CoE № 1834 от октября 2011 года и Рекомендация Парламентской ассамблеи № 1980 от октября 2011 года под общим названием «Борьба с оборотом материалов, изображающих насилие над детьми, при помощи целенаправленных, комплексных и согласованных международных усилий». Они сфокусированы на:

— создании эффективных механизмов по пресечению любого рода распространения через Интернет материалов с насилием над несовершеннолетними, с допущением блокировки веб-сайтов;

— обучении детей навыкам самозащиты, в том числе работе с информационными ресурсами.

Кроме того, говоря об инициативах CoE, необходимо упомянуть Стратегию по правам ребенка на 2016–2021 года, принятую в Софии в апреле 2016-го. Она была разработана созданным специально для этих целей Комитетом экспертов по стратегии Совета Европы в области прав ребенка.

В документе отмечается, что дети имеют право на обучение, досуг и общение в Интернете, будучи защищенными от запугивания, радикализации, сексуального насилия и других рисков. Стратегия призвана ориентировать национальные правительства на создание эффективных механизмов обеспечения безопасности несовершеннолетних в онлайн-пространстве.

Также достойна внимания Рекомендация № 7 Комитета министров CoE о руководящих принципах уважения, защиты и соблюдения прав детей в цифровой среде от июля 2018 года. Она не является обязательной для государств-членов, однако дает необходимые ориентиры для их правительств. В ее подготовке участвовали международные организации, бизнес-сообщества и национальные структуры, ответств ные за благополучие детей на европейском пространстве.

ОПЫТ СТРАН

ВЕЛИКОБРИТАНИЯ

В Великобритании в сентябре 2020 года был разработан Свод правил по возрастному проектированию, или Детский кодекс, направленный на защиту конфиденциальности несовершеннолетних. Он состоит из основанных на оценке риска 15 стандартов, которых должны придерживаться все онлайн-сервисы страны. Исходя из кодекса, цифровым платформам следует:

— по умолчанию использовать наиболее безопасные настройки конфиденциальности, автоматически отключать, например, такие

функции, как отслеживание местоположения;

— избегать практики сбора данных о ребенке для того, чтобы использовать эту информацию для удержания на ресурсе продолжительное время;

Как сообщается на портале Всемирного экономического форума, молодые люди легко обходят меры по проверке возраста при регистрации на ряде онлайн-ресурсов. Дело в том, что кодекс устанавливает требования к цифровым платформам по защите детей в Интернете, но не предписывает механизмы проверки возраста пользователей.

Бизнес-платформа Statista приводит список видов потенциальных рисков в социальных сетях. Он основан на мнении британских детей в феврале 2020 года. Опасности указываются, начиная с наиболее упоминаемых групп:

— нежеланные друг, подписка, контакт;

— люди, притворяющиеся кем-то другим;

— запугивание, оскорбительное поведение;

— преследование, киберпреследование;

— личная информация стала общедоступной;

— разжигание ненависти;

— троллинг;

— принуждение к отправке фотографий, видео, информации;

— контент, пропагандирующий членовредительство;

— фейковые новости;

— поддельные изображения, видео;

— оскорбительные изображения, видео.

Также, по данным Statista, по состоянию на февраль 2020 года, 71 % британских детей не сообщали взрослым об ознакомлении в Сети с оскорбительным или вредоносным контентом. 17 % несовершеннолетних не говорили об этом, так как не считали попавшие в поле зрения материалы достаточно плохими. А другие 17 % отписывались от такого онлайн-контента или блокировали его, вместо того чтобы заявить о нем. При этом 14 % респондентов не думали, что рассказ о произошедшем поможет, а 12 % — и вовсе не знали, что делать.

Если рассматривать оценку степени надежности защиты онлайн-платформ от вредоносного контента, по состоянию на февраль 2020 года, по данным Statista, 73 % британских детей доверяли новостному агентству BBC News в плане ограждения от вредоносных или жестоких материалов. 57 % респондентов находили безопасным сервис обмена мгновенными сообщениями Google Hangouts, а 55 % — его конкурента WhatsApp. И только 40 % опрошенных называли соцсеть TikTok.

Кроме того, согласно онлайн-опросу, проведенному в Великобритании в феврале 2020 года, 30 % детей, которые использовали платформу Facebook, столкнулись с потенциальными рисками на ней. 17 % респондентов сообщили, что подверглись онлайн-вреду в Instagram, а 10 % — в Twitter.

17 марта 2022 года в Парламент Великобритании был внесен законопроект о безопасности в Интернете. В документе предусмотрены строгие меры, в частности:

— предотвращение распространения детской порнографии, террористических материалов и информации о преступлениях на почве ненависти;

— требование к крупным цифровым платформам об ограждении детей от законного, но вредоносного контента.

Также стоит отметить, что в Великобритании функционирует ряд организаций для консультирования родителей. Их специалисты объясняют, как лучше рассказывать детям о рисках в Сети. К таким структурам относятся:

— Центр безопасного Интернета;

— Учебный центр телекоммуникационной компании Telenor;

— Платформа электронного обучения фонда Stairway.

ГРЕЦИЯ

Правительство Греции в структуре Отдела полиции по борьбе с киберпреступностью создало Подразделение цифровых расследований и защиты несовершеннолетних в Интернете. Оно имеет доступ к базе данных Interpol о сексуальной эксплуатации детей по всему миру, в его штате работает психолог для консультирования жертв и их родителей, а также у него есть круглосуточная горячая линия для обращений за помощью и электронная почта для подачи жалоб. Кроме того, Отдел полиции по борьбе с киберпреступностью совместно с Министерством внутренних дел Греции запустил информационно-просветительские портал и мобильное приложение Cyberkid. Данные

ресурсы предоставляют советы для всей семьи о безопасном использовании Интернета.

Также стоит отметить, что в Греции, согласно законодательству, интернет-провайдеры обязаны добавлять сайт-нарушитель в черный список доменных имен по постановлению суда или представлению прокурора. Основанием для удаления или блокировки ресурсов может стать наличие на них материалов о сексуальном насилии над детьми.

В дополнение ко всем вышеописанным инициативам нужно сказать, что в стране функционирует Центр безопасного Интернета. Он издает пособия по дезинформации и риторике ненависти для школьников и преподавателей, а также запустил справочно-информационный портал для семей и представителей образовательной системы SaferInternet4Kids, линию помощи Help-Line и форму для жалоб SafeLine по вопросам онлайн-безопасности.

ИНДИЯ

В 2005 году Индия подписала два протокола к Конвенции ООН о правах ребенка —об участии несовершеннолетних в вооруженных конфликтах и о торговли детьми, детской проституции и порнографии. Тем самым власти подтвердили стремление защищать несовершеннолетних ото всех форм эксплуатации, произвольного или незаконного вмешательства в их частную жизнь. Также были приняты меры по ослаблению шифрования в связи с неправомерным использованием социальных сетей для совершения преступлений и сексуальной эксплуатацией детей в Интернете.

Согласно исследованию американского разработчика антивирусного программного обеспечения McAfee, 89 % индийцев считают, что школы должны обучать детей безопасности в Интернете. Из них 62 % полагают, что курс по цифровому благополучию необходимо внедрять в программу отдельной дисциплиной, а 27% — что его следует интегрировать в предмет информатика.

Комиссия по университетским грантам Индии разработала Справочник по цифровой гигиене для высших учебных заведений. Одна из его основных целей — обеспечить студентов и преподавателей безопасным киберпространством в классах. Для ее реализации в документе советуют:

— использовать функцию «безопасный просмотр» при открытии веб-страниц;

— отключать веб-камеры и звук компьютеров без надобности их использования;

— не загружать контент при подключении к общедоступному Wi-Fi;

— отказаться от менеджера паролей.

— Стоит отметить, что во время пандемии COVID-19 такой справочник стал невероятной необходимостью для учителей и учащихся. Для повышения цифровой грамотности в нем советуется:

— строжайше настроить конфиденциальность в соцсетях;

— установить надежный антивирус;

— не загружать разного рода материалы с ненадежных ресурсов;

— не разглашать в Сети финансовую информацию;

— систематически очищать историю просмотров и кеш браузера;

— регулярно обновлять мобильные приложения;

— избегать поддельных сайтов, в том числе с предложениями трудоустройства.

Также в справочнике рассмотрены ключевые киберпреступления, среди которых —социальная инженерия, дезинформация, пропаганда, дипфейки, кража личных данных, шпионаж и фишинг.

ИРЛАНДИЯ

В Ирландии действуют сразу несколько национальных тематических центров:

— Научно-исследовательский центр борьбы с буллингом;

— Официальный центр онлайн-безопасности Be Safe Online;

— Информационный центр безопасности в Сети Webwise.

В ноябре 2021 года Департамент туризма, культуры, искусства, Гэлтахта, спорта и СМИ Ирландии провел Национальное исследование безопасности детей и взрослых в Сети. Оно выявило существенные различия в онлайн-защищенности несовершеннолетних в разных возрастных группах: 9–10, 11–12, 13–14 и 15–17 лет — и стало точкой отсчета для наработок по вопросам разнообразного подхода к восприятию цифровой среды детьми и их родителями. На основе отчетов исследования в дальнейшем планируется сформировать эффективную государственную политику по безопасности в Интернете.

Также в декабре 2020 года Комиссия по защите данных Ирландии подготовила документ «Основы ориентированного на детей подхода к обработке данных». Его целью стало создание стандартов для бизнеса. В тексте эксперты привели 14 необходимых для соблюдения основ по усилению защиты несовершеннолетних при обработке их персональных данных. Исходя из них, поставщикам онлайн-услуг следует:

— обеспечить минимально необходимым уровнем защиты всех пользователей, если только не применяется основанный на оценке риска подход к проверке их возраста (раздел 1.4 «Соблюдение основ»);

— получить осознанное, в виде четкого заявления или других конкретных действий, согласие на обработку личных данных (раздел 2.4 «Правовые основы для обработки данных детей»);

— добиться, чтобы преследование законных интересов при обработке частной информации о детях не противоречило их правам и не оказывало негативного влияния на них (раздел 2.4 «Правовые основы для обработки данных детей»);

— предпринимать шаги для идентификации пользователей и обеспечить безопасность всех услуг для детей (раздел 3.1 «Знание аудитории»);

— предоставлять несовершеннолетним информацию об обработке данных при каждом запросе, даже если согласие на нее было получено от их родителей (раздел 3 «Прозрачность и дети»);

— отчитываться об использовании личной информации в краткой и понятной форме с учетом возраста ребенка (раздел 3 «Прозрачность и дети»);

— не забывать о правах детей на использование личной информации для удовлетворения интересов (раздел 4.1 «Положение детей как правообладателей»);

— не использовать полученное от несовершеннолетних согласие на обработку данных в качестве оправдания обращения с ними, как со взрослыми (раздел 5.1 «Возраст цифрового согласия»);

— регулярно доказывать эффективность мер по защите данных детей (раздел t5.2 «Проверка согласия родителей»);

— не лишать пользовательского опыта несовершеннолетних простым ограничением ресурса, хотя бы отчасти ориентированного на детскую аудиторию (раздел 5.4 «Подтверждение возраста и пользовательский опыт ребенка»);

— не полагаться на теоретические пороговые возрастные значения для доступа к услугам при соблюдении обязательств общего регламента по защите данных детей (раздел 5.5 «Минимальный возраст пользователей»);

— не использовать персональную информацию несовершеннолетних в маркетинговых или рекламных целях из-за особой восприимчивости детей, за исключением случаев, когда имеется четкое доказательство благостного эффекта (раздел 6.2 «Профилирование и автоматизированное принятие решений»);

— проводить оценку воздействия на защиту данных для сведения к минимуму рисков их обработки (раздел 7.1 «Оценка воздействия на защиту данных»);

— включать систему защиты информации во все услуги для детей (раздел 7.2 «Защита данных по умолчанию»).

Также ранее упомянутый информационный центр безопасности в Сети Webwise реализует в Ирландии проект «Безопасный Интернет», который объединяет ИТ-отрасль, сектор образования, службу защиты детей и правительство. Инициатива частично финансируется одноименной программой Евросоюза. В нее включены:

— создание устойчивой к развитию технологий системы скоординированных национальных действий по обеспечению безопасности в Интернете;

— разработка ресурсов повышения информированности детей, родителей и учителей о преимуществах и рисках Интернета;

— обеспечение работы круглосуточной консультационной службы по онлайн-безопасности в соответствии с высочайшими профессиональными стандартами.

— Кроме того, Webwise выступает в Ирландии в качестве технического координатора по тематических вопросам. В него входит ряд объединений:

— Ассоциация интернет-провайдеров Ирландии принимает сообщения общественности о подозрительном и незаконном онлайн-контенте.

— Ирландское общество по предотвращению жестокого обращения с детьми круглосуточно и без выходных предоставляет услуги несовершеннолетним.

— Национальный совет родителей начальной школы помогает семьям решать разного рода неприятные ситуации, возникшие в Сети.

США

В 1998 году Конгресс США принял Закон о защите конфиденциальности детей в Интернете (Children's Online Privacy Protection Act, COPPA). В связи с этим Федеральная торговая комиссия США издала правила конфиденциальности несовершеннолетних в Сети и начала следить за их соблюдением.

COPPA гарантирует родителям контроль над тем, какую информацию веб-сайты могут собирать об их детях. Пять основных пунктов закона обязывают компании:

— Анализировать аудиторию для достойного обращения с ней. Так, ресурс для детей от 13 лет не должен блокироваться для пользователей младше, если он вполне ориентирован на них.

— Четко осознавать, что представляет собой персональная информация. Например, фотографии, голосовые записи и видео являются личными данными.

— Размещать ссылку на политику конфиденциальности на стартовом экране мобильных приложений.

— Обзаводиться надлежащим уровнем родительского согласия. Недостаточно отправить представителю несовершеннолетнего электронное письмо с сообщением о том, что ребенок заинтересован в подписке на онлайн-сервис. Во избежание нарушения уведомление должно содержать всю необходимую информацию с актуальными ссылками.

— Запрашивать согласие на добавление новых функций. При этом необходима уверенность в актуальности политики конфиденциальности. Многие компании обновляют контент, но забывают о разделах сбора и использования личной информации.

— COPPA применяется только к ресурсам для детей. Поэтому закон приводит ряд факторов для определения необходимости его соблюдения. Возрастному анализу должны подвергаться:

— предмет;

— визуальный контент;

— анимированные персонажи;

— мероприятия и стимулы;

— аудиоконтент;

— возраст моделей;

— направленность обращений от лица знаменитостей;

— язык;

— реклама;

— эмпирические данные о составе пользователей;

— доказательства относительно целевой аудитории.

Закон США о защите детей в Интернете от декабря 2000 года требует от финансируемых государством школ и библиотек фильтровать онлайн-контент. Согласно постановлению, дети не должны встречаться с непристойными и вредными материалами на школьных или библиотечных компьютерах.

Также в 2018 году в США был принят Закон о борьбе с торговлей людьми в целях сексуальной эксплуатации в Интернете. Таким образом наконец были получены юридические инструменты для поиска веб-сайтов, сознательно способствующих секс-торговле и исторически служивших онлайн-борделями для сутенеров.

Кроме того, в ряде штатов США действуют законы о кибербуллинге, а во всех штатах — законы, требующие от школ реагировать на издевательства. В некоторых штатах даже есть положения по борьбе с травлей при ее влиянии на успеваемость в учебном заведении. Более подробная информация о политике каждого штата представлена на портале исследовательского центра Cyberbulling.

В 2001 году Национальный центр без вести пропавших и эксплуатируемых детей США создал ресурс NetSmartz для информирования семей о безопасности в Интернете. На портале, в частности, можно найти материалы о том, как начать разговор с несовершеннолетними о защищенности в Сети.

В 2010 году одна из ведущих американских организаций по безопасности в Интернете Enough Is Enough запустила национальную программу Internet Safety 101SM. Она представляет собой комплексный мультимедийный подход по об-

учению родителей защите детей от онлайн-угроз. Так, к примеру, на портале программы есть список правил по безопасности в Сети.

В июне 2021 года члены Сената и Конгресса США призвали американские цифровые компании добровольно принять британский Свод правил по возрастному проектированию. Власти заявили, что бизнес обязан ставить благополучие молодых пользователей на первое место, независимо от их места жительства.

В марте 2022 года американский президент Джо Байден призвал Конгресс США ввести более строгие правила конфиденциальности детей, запретить целевую рекламу для несовершеннолетних и оказать давление на разработчиков соцсетей, чтобы они проектировали продукты с учетом безопасности детской аудитории.

СЕРБИЯ

Вопросы защищенности детей в онлайн-среде находятся в фокусе повестки сербских властей. В 2016 году Национальное собрание страны приняло Закон об информационной безопасности, а Правительство Сербии — Положение о защите детей при использовании ИКТ.

С 2017 по 2019 год Сербия проводила в 19 европейских странах исследование и в 2020-м представила его результаты в отчете «Дети Евросоюза в цифровой среде». Целью опросов было выявить схожести и отличия в использовании несовершеннолетними разного возраста сетевых коммуникаций. В частности, было установлено, что дети от 11 до 12 лет чувствуют себя компетентными в Интернете. Авторы исследования полагают, что это связано с внедрением в их школьную программу информатики как обязательного предмета.

Также стоит отметить, что Бюро по правам человека и сексуальных меньшинств Сербии в Комментариях Республики к Замечаниям общего порядка № 25 ООН о правах детей в связи с цифровой средой заявило, что для снижения интернет-зависимости, помимо повышения онлайн-грамотности, следует заниматься ее активной профилактикой.

По мнению экспертов, только тогда риски и вред цифровой среды не будут преобладать над преимуществами ее использования.

В феврале 2017 года при Министерстве торговли, туризма и телекоммуникаций Сербии был создан Национальный контактный центр по безопасности детей в Интернете. Он стал центральной системой страны по обучению несовершеннолетних способам защиты при использовании цифровых технологий и по консультированию семей на темы, связанные с данной проблематикой.

Также сербский Центр по правам ребенка разработал цифровую платформу «Твое право», адаптированную для детей. На ней содержится актуальная информация о профилактике надругательств над несовершеннолетними в Интернете, а также об их защите от данного вида преступлений. Платформа информирует детей о практиках, которые могут помочь в распознании онлайн-рисков, а также дает советы по реакции на опасность и сообщает, куда обращаться за помощью.

Центр безопасного Интернета Сербии, основанный в январе 2013-го, в рамках проекта Click Safely, финансируемого Европейским союзом и телекоммуникационной компанией Telenor, дважды в год в разных городах страны организует серию информационных мероприятий для детей от 11 до 17 лет, их родителей, педагогов, школьных психологов и представителей министерства образования. На них разъясняются угрозы, связанные с кибербуллингом, материалами с сексуальным насилием над детьми, фишингом, онлайн-хищниками, разжиганием ненависти и другими онлайн-рисками. Также на мероприятии эксперты обучают слушателей основам сетевого этикета, защиты персональных данных, настройки конфиденциальности и тому подобного.

Кроме того, в августе 2013 года Центр безопасного Интернета Сербии запустил бесплатную горячую линию «Сетевой патруль» (Net Patrola), которая, как и создавшая ее организация, является членом объединенной сети Insafe and INHOPE Центров безопасного Интернета в Европе. Ее специалисты круглосуточно и без выходных принимают и обрабатывают сообщения от детей о незаконном или вредоносном контенте в Интернете, а также о злонамеренном поведении в Сети. С 2016 года ежедневно, кроме нескольких технических часов в неделю, консультацию и поддержку могут получить и родители несовершеннолетних.

Также Министерство образования, науки и технологического развития Сербии и Центр по правам ребенка в Ужице разработали первый цифровой справочник на сербском языке — «Дети и Интернет: разумно с самого начала». Руководство по онлайн-безопасности предназначено для несовершеннолетних, родителей и наставников. Пособие состоит из трех разделов

— «Темы», «Викторина» и «Ресурсы». В нем можно найти четыре тематических мультфильма, словарь цифрового века, брошюру для родителей, рекомендации по безопасному и конструктивному использованию онлайн-технологий и Интернета и другие полезные материалы.

Примечательно и то, что в октябре 2016 года около 70 сотрудников полиции со всей Сербии приняли участие в тренинге Europol «Борьба с сексуальной эксплуатацией детей в Интернете». В течение десяти дней правоохранители повышали квалификацию, перенимая опыт ведущих специалистов в области борьбы с киберпреступностью.

Также Сербия принимает участие в двух аналитических проектах Evropol с международными контактными пунктами. Так, проект Cyborg направлен на борьбу с киберпреступностью, а проект Twins нацелен на искоренение детской порнографии.

Кроме того, Судебная академия Сербии при поддержке международной организации Save the Children разработала для судей, прокуроров страны и их помощников программу однодневного Тренинга по киберпреступности и защите несовершеннолетних. В ходе его реализации также было подготовлено тематическое руководство.

ЕВРОПЕЙСКИЙ СОЮЗ

25 мая 2018 года вступил в силу Общий регламент защиты персональных данных Европейского парламента и Совета Европейского союза. Впервые в законодательной практике Евросоюз признал особые риски для детей при сборе и обработке их личной информации без надлежащих гарантий, а также их право на ее защиту. Кроме того, регламент призвал информировать несовершеннолетних о процессах работы с их персональными данными.

В январе 1999 года Европейский парламент и Совет Евросоюза запустили многолетний План действий Сообщества по содействию более безопасному использованию Интернета путем борьбы с незаконным и вредоносным контентом. В частности, в нем ставился вопрос о защищенности детей в онлайн-среде. С 2015 года цели плана финансируются Фондом объединения европейских инфраструктур (Connecting Europe Facility, CEF).

CEF поддерживает развитие высокопроизводительного, устойчивого и взаимосвязанного взаимодействия в сферах транспорта, энергетики и цифровых услуг. В частности, программа стимулирует деятельность в европейских странах сети Центров безопасного Интернета (Safer Internet Centres).

В 2013 году в Евросоюзе была опубликована Рамка цифровой компетентности для граждан (European Digital Competence Framework for Citizens, DigComp). В 2017-м новая версия документа — DigComp 2.1 — включила в себя восемь уровней квалификации, от базового до узкоспециализированного. Это поспособствовало разработке материалов для обучения, а также помогло в создании инструментов для оценки развития цифровых компетенций граждан.

В марте 2022 года была издана еще одна версия — DigComp 2.2. В нее включили более 250 новых знаний, направленных на помощь гражданам в овладении навыком уверенного, критического и безопасного взаимодействия с новейшими цифровыми технологиями.

В качестве дополнений в Евросоюзе были разработаны Рамки цифровых компетенций для преподавателей (DigCompEdu) и образовательных организаций (DigCompOrg), а также для предпринимателей (EntreComp), индивидов и социума (LifeComp). В частности, для цифровых возможностей школ был создан бесплатный онлайн-инструмент для самостоятельного анализа — SELFIE.

Кроме того, в июле 2021 года Европейский парламент и Совет Евросоюза приняли Регламент о временном отступлении от некоторых положений Директивы в отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи от июля 2020-го с целью борьбы с сексуальным насилием над детьми в Интернете.

В июне 2022 года для Общего регламента защиты персональных данных Европейского парламента и Совета Евросоюза были предложены новые правила по предотвращению сексуального онлайн-насилия над детьми и борьбе с ним.

В представленный текст были включены:

— Обязательная оценка рисков и меры по их снижению. Поставщики цифровых услуг должны определять вероятность незаконного использования их продуктов и способствовать уменьшению степени их опасности.

— Необходимость целевого обнаружения. Ответственным за пересмотр оценки рисков следует назначить определенный госорган. При выявлении опасности он будет обращаться в суд за ордером на об-

наружение незаконных материалов.

— Строгие меры предосторожности при обнаружении. В процессе обнаружения провайдеры должны использовать исключительно индикаторы Центра экспертизы Европы, который тоже должен быть создан в рамках реализации предложенных правил.

— Также необходимо отдавать предпочтение технологиям, которые несут наименьшие риски для конфиденциальности и наиболее защищены от ложных срабатываний.

— Строгие обязательства по предоставлению отчетности. Провайдеры при обнаружении сексуального насилия над детьми в Интернете должны незамедлительно сообщить об этом в Центр экспертизы Европы.

— Эффективное удаление. Когда злонамеренные материалы не могут быть быстро удалены из Сети, например, если они размещены за пределами Евросоюза, национальные власти должны издать приказ об их изъятии, а провайдеры — отключить возможность просматривать их.

— Блокировка лазеек для груминга. Магазины приложений должны гарантировать невозможность загрузки детьми продуктов, которые могут подвергнуть их высокому риску.

— Надежные механизмы контроля. Центр экспертизы Европы должен проверять сообщения о потенциальном сексуальном онлайн-насилии над детьми, прежде чем делиться материалами с правоохранительными органами.

— Открытость к оправданию. Провайдеры и интернет-пользователи должны иметь право оспорить любую меру в суде.

Также в предложенных правилах отдельно указаны функции Центра экспертизы Европы:

— поддерживать базу индикаторов: хеш-классификаторов и классификаторов интеллектуальных систем;

— получать сообщения о возможном онлайн-насилии над детьми, оценивать их и передавать правоохранительным органам;

— проводить профилактические меры;

— оказывать помощь жертвам;

— способствовать обмену передовым опытом между государствами-членами Евросоюза;

— сотрудничать с партнерами за пределами Евросоюза, учитывая глобальный характер таких преступлений.

Стоит также отметить, что в Евросоюзе функционирует портал Better Internet for Kids, на котором предоставляется информация по вопросам улучшения цифровой среды для детской аудитории от объединенной сети Insafe and INHOPE Центров безопасного Интернета в Европе и других ключевых заинтересованных сторон. Основная задача портала — развивать цифровую грамотность среди несовершеннолетних, родителей и учителей. Также он борется с материалами о сексуальном насилии над детьми через сеть горячих линий INHOPE.

Кроме того, европейский Центр цифрового образования разработал «Колесо цифровых компетенций». Оно предоставляет обзор необходимых навыков, а также дает конкретные рекомендации по их приобретению.

ИНИЦИАТИВЫ ПРАВОЗАЩИТНЫХ И ИССЛЕДОВАТЕЛЬСКИХ ОРГАНИЗАЦИЙ

Ресурсы и инструменты для защиты детей можно условно разделить на 3 большие группы:

— защита от кибербуллинга;

— защита от секстинга;

— мониторинг онлайн-действий ребенка.

В настоящее время разработан и используется целый ряд программных продуктов, которые облегчают контроль за детьми в Сети. Это обусловлено тем, что, как правило, уровень цифровой грамотности родителей не всегда позволяет своевременно выявить угрозы для ребенка и противостоять им.

Ниже приведены подходы и практики 7 организаций.

В Приложении № 1 обзора дополнительно дан перечень более десяти ключевых инициатив правозащитных и исследовательских организаций и их краткое описание.

АССОЦИАЦИЯ СТАНДАРТОВ ИНСТИТУТА ИНЖЕНЕРОВ ПО ЭЛЕКТРОТЕХНИКЕ И ЭЛЕКТРОНИКЕ (IEEE)

Международная Ассоциация стандартов Института инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineers, IEEE) в ноябре 2021 года опубликовала Стандарт 2089–2021 для цифровых платформ по соответствию услуг возрасту. В документе представлены рекомендации по выявлению онлайн-рисков, приведению цифро-

вых услуг в должное относительно жизненной зрелости пользователей состояние, а как следствие, снижению уровня их опасности для детей. Стандарт сосредоточен на нескольких ключевых областях, среди которых — следующие:

— признание факта о наличии детской аудитории;

— приверженность защите прав несовершеннолетних;

— создание подходящих детям условий;

— предоставление информации в соответствии с возрастом;

— приоритизация интересов детей над коммерческими целями.

Примечательно, что в 2021 году Ассоциация стандартов IEEE издала еще один важный документ — Стандарт 7000–2021 для решения этических проблем при проектировании цифровых платформ. Как было отмечено в журнале IEEE Spectrum, такие стандарты способствуют коллективному построению лучшего и безопасного цифрового мира для детей.

Также в июле 2020 года Ассоциация стандартов IEEE разработала Советы по безопасности для детей при кибербуллинге. По мнению специалистов, родителям следует:

— поощрять открытое общение: ребенок должен знать, что взрослый всегда рядом, что бы ни случилось;

— использовать приложения для родительского контроля, чтобы отслеживать сообщения ребенка, его местоположение и времяпрепровождение в Интернете;

— не решать все за ребенка, когда над ним издеваются: одна из целей кибербуллинга — лишение достоинства и уверенности в себе, поэтому важно привлекать несовершеннолетнего к поиску выходов;

— объяснить, что ни при каких обстоятельствах ребенок не должен раскрывать свои пароли, полное имя, место проживания, возраст и другую личную информацию;

— посоветовать ребенку не заполнять онлайн-анкеты с подробными сведениями о себе, чтобы данные не попали в руки злоумышленников.

НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ENOUGH IS ENOUGH (EIE)

Одна из ведущих американских некоммерческих организаций по безопасности в Интернете Enough is Enough (EIE) с 1994 года ведет борьбу за менее рискованное использование Сети детьми и родителями. Она разрабатывает и продвигает профилактические решения для сохранения равенства людей и уважения человеческого достоинства, в которых призывает к ответственности общественность, ИТ-отрасль и юридическое сообщество.

Кроме того, EIE регулярно оснащает детей и родителей информацией о новейших онлайн-угрозах и сотрудничает с Конгрессом США по совершенствованию контроля над крупнейшими американскими компаниями в индустрии информационных технологий, которые так или иначе получают прибыль от уязвимости детей в онлайн-среде.

В 2022 году EIE присоединилась к Коалиционному письму из более чем 100 организаций и защитников детей в поддержку законопроекта EARN IT от 2020-го об устранении злоупотреблений интерактивными технологиями.

Текущая повестка EIE направлена на:

— продвижение национальных усилий по обеспечению безопасности в Интернете;

— расширение кампании «Безопасный WiFi», которая призывает американский частный сектор фильтровать информацию, предоставляемую через общедоступные сети,

— на предмет онлайн-рисков;

— утверждение новой политики, которая повысит ответственность технологической отрасли за распространение материалов с сексуальным насилием над детьми, случаи соблазнения и сексуальной торговли.

ЕВРОПЕЙСКАЯ ИНИЦИАТИВА SAFE ONLINE

Основное внимание европейской инициативы Safe Online направлено на повышение уровня медиаграмотности детей посредством ее всестороннего освоения родителями. Данная инициатива координируется и поддерживается образовательными учреждениями и ассоциациями по всей Европе. Благодаря ей тысячи родителей стали лучше понимать онлайн-деятельность, больше узнали о возможностях Интернета и повысили свою информированность о его рисках.

Кроме того, Safe Online способствует глобальным политическим дискуссиям о безопасно-

сти детей в Сети и содействует накоплению международных знаний об этой проблеме.

АЛЬЯНС IKEEPSAFE

Американский некоммерческий альянс iKeepSafe, основанный в 2005 году, предоставляет сертификаты конфиденциальности данных технологическим компаниям и образовательным ресурсам с последующей консультационной поддержкой. Основная миссия объединения заключается в обеспечении безопасного цифрового ландшафта для семей и ученых заведений.

Так, программа сертификации iKeepSafe «Безопасная гавань» гарантирует, что методы сбора, использования, хранения и раскрытия личной информации детей соответствуют принципам и требованиям COPPA. Компании, соблюдающие закон, награждаются значком. Это позволяет родителям и школам легко идентифицировать достоверно безопасные продукты.

Также iKeepSafe, объединяя более ста политических лидеров, прокуроров, преподавателей, сотрудников правоохранительных органов, технических экспертов и специалистов в области общественного здравоохранения, отслеживает глобальные тенденции, связанные с цифровыми продуктами и их влиянием на детей. Кроме всего прочего, это способствует информированию сообщества о рисках и их предотвращении при использовании несовершеннолетними новейших онлайн-технологий. На портале iKeepSafe содержатся различные руководства к действию по созданию безопасной детской цифровой среды для родителей, преподавателей и производителей.

МЕЖДУНАРОДНАЯ ЛИНИЯ ПОМОЩИ ДЕТЯМ (CHILD HELPLINE INTERNATIONAL)

Международная линия помощи детям (Child Helpline International, CHI), основанная в 2003 году, включает в себя 160 организаций из 140 стран. CHI ежегодно оказывает помощь десяткам миллионов детей, нуждающихся в поддержке и защите, поддерживает создание и укрепление телефонных линий доверия для несовершеннолетних по всему миру и анализирует полученные данные для выявления пробелов в системах защиты детей.

Также CHI предоставляет детям и родителям рекомендации по столкновению

с онлайн-рисками разного рода, среди которых:

— кибербуллинг;

— дискриминация и разжигание ненависти;

— груминг;

— незаконный и неприемлемый контент;

— нарушение конфиденциальности;

— сексуальные вымогательство и домогательство;

— неприятные контакты с незнакомцами.

ФОНД НАБЛЮДЕНИЯ ЗА ИНТЕРНЕТОМ (IWF)

Фонд наблюдения за Интернетом (Internet Watch Foundation, IWF) был создан в Великобритании в 1996 году. Сегодня он позиционирует себя одним из мировых лидеров в борьбе с сексуальным насилием над несовершеннолетними в Сети. IWF уделяет большое внимание международному сотрудничеству и работает с технологическим сообществом, правительствами, правоохранительными органами и службами экстренной помощи по всему миру. Приоритетный проект фонда — горячая онлайн-линия, посредством которой можно анонимно отправить специалистам материалы сексуального насилия над детьми в Интернете для их последующего удаления. В 2021 году благодаря ей были приняты меры в отношении более 250 тысяч сайтов с незаконным контентом.

Еще одним важным инструментом IWF является интеллектуальный поисковый робот. Он использует новаторскую технологию для сканирования веб-страниц в Интернете в поисках изображений и видео, демонстрирующих сексуальное насилие над детьми, для их последующего удаления. Только в 2021 году поисковый робот просканировал почти 14 миллиона веб-страниц и более 66 миллионов изображений.

Также стоит отметить, что больше 170 компаний, включая цифровых гигантов, являются членами IWF. Членство в фонде дает эксклюзивный доступ к его инструментам, таким как:

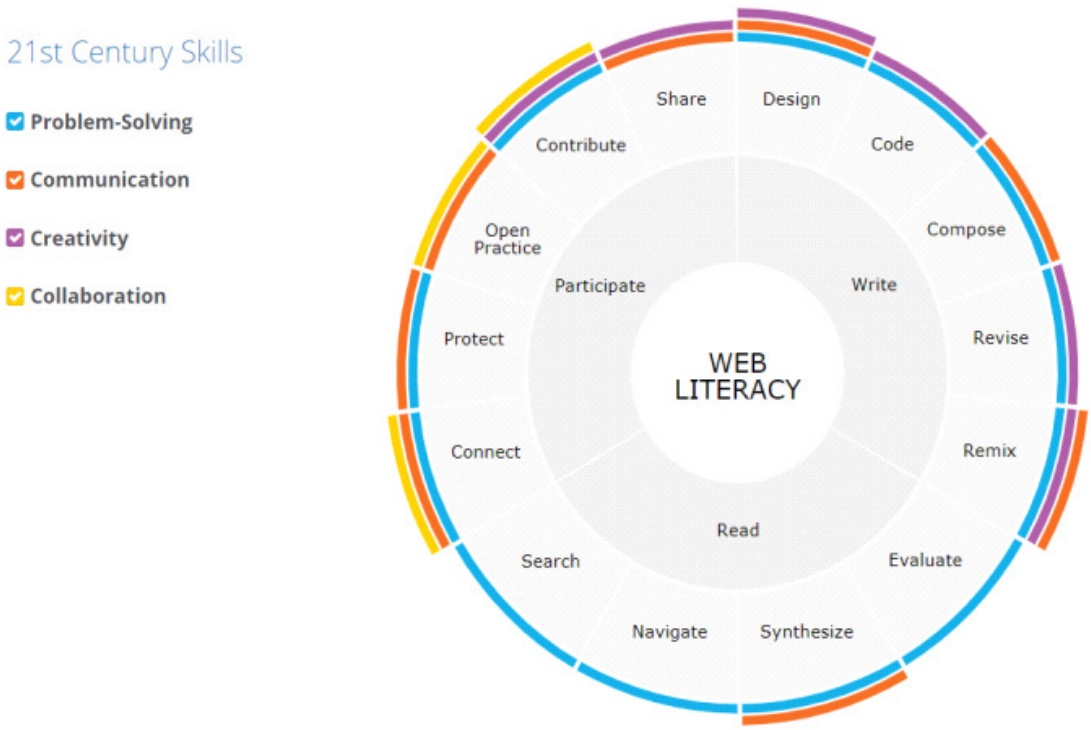
— список онлайн-ресурсов с материалами сексуального насилия над детьми;

— список ключевых слов, фраз и кодов, которые злоумышленники используют для сокрытия незаконных фото и видео;

— уведомления о необходимости незамедлительного удаления материалов, подозреваемых в наличии CSAM, и не только.

Кроме того, IWF занимается просветительской деятельностью. Так, например, сервис дает рекомендации родителям о разговоре с детьми об опасностях в Сети.

Рисунок № 3



Источник: блог Mozilla «dist://ed»

По мнению специалистов фонда, необходимо:

— поговорить с ребенком о сексуальном насилии в Интернете, выслушать его опасения;

— согласовать основные правила использования онлайн-технологий всей семьей;

— узнать о ресурсах, которые ребенок использует регулярно;

— освоить инструменты для обеспечения его онлайн-безопасности.

ГЛОБАЛЬНЫЙ АЛЬЯНС WEPROTECT

Международный альянс WePROTECT представляет собой комбинацию двух глобальных инициатив:

— Европейской комиссии и Министерства юстиции США против сексуального насилия над детьми в Интернете;

— Правительства Великобритании в борьбе с идентичной проблемой.

В феврале 2018 года на Саммите по поиску решений прекращения насилия над детьми в Швеции WePROTECT представил Глобальную систему оценки угроз — первое в истории исследование факторов уязвимости несовершеннолетних к риску сексуальных эксплуатации и насилия. Система показала, что такого рода злодеяния сегодня являются наиболее коварной формой киберпреступности, а современные технологии предоставляют правонарушителям беспрецедентные возможности для жестокого обращения с детьми в массовом масштабе.

Кроме того, стоит отметить, что в основе Стратегии WePROTECT от июля 2016 года по борьбе с данной проблемой лежит поддержка стран в разработке скоординированных ответных мер с участием многих заинтересованных. Именно поэтому в том же году альянс опубликовал Модельные национальные ответы (Model National Response, MNR), с помощью которых правительства и другие стейкхолдеры могут проверить, все ли шаги они предпринимают для защиты несовершеннолетних в Сети.

Так, в докладе WePROTECT «Создавая будущее» сообщается о том, как именно MNR поддерживают национальные усилия по прекращению жестокого обращения с детьми в Интернете. С примерами опыта стран в реализации MNR также можно ознакомиться в специальном

отчете альянса. Документируя передовую практику и извлеченные уроки, он иллюстрирует, как MNR стал ключевым ориентиром для поддержки разработки скоординированных и всеобъемлющих национальных мер.

ПРАКТИКИ В ОБЛАСТИ ЦИФРОВОЙ ГРАМОТНОСТИ, ЦИФРОВОЙ ГИГИЕНЫ И ЦИФРОВОГО БЛАГОПОЛУЧИЯ

В августе 2019 года UNICEF представила результаты исследования цифровой грамотности детей. Оно проводилось для определения уровня существующих онлайн-компетенций несовершеннолетних, выделения значимых политик и практик в области обучения навыкам онлайн-среды и составления рекомендаций по их адаптации к новейшим потребностям.

На Всемирном образовательном форуме в Инчхоне в 2015 году отмечалась важность обучения педагогов использованию информационно-коммуникационных технологий для укрепления образовательных систем и эффективного обучения несовершеннолетних. В OECD тоже считают, что дети часто понимают технологии лучше, чем взрослые, поэтому преподавателям необходимо стремиться к повышению уровня цифровых знаний. Так, при разработке школьной политики, по мнению специалистов OECD, важно:

— информировать учителей об онлайн-рисках для помощи несовершеннолетним в управлении ими;

— объяснять педагогам недопустимость публикации материалов о детях без их разрешения;

— стимулировать детей переходить с просмотра контента на его создание;

— преодолевать цифровой разрыв, обучая несовершеннолетних из неблагополучных семей навыкам онлайн-мира.

— В блоге некоммерческой организации Mozilla, создавшей одноименный браузер, представлена карта веб-грамотности XXI века (рисунок № 3):

Цифровой журнал Equip выделяет несколько аспектов онлайн-жизни при применении цифровых инструментов:

— эксплуатация;

— потребление информации;

— решение определенных задач;

— общение и сотрудничество.

Кроме того, Equip указывает на важность законного и этичного поведения при использовании технологий.

Стоит также отметить, что в интернет-среде сейчас активно поднимается и вопрос цифрового благополучия, в частности связанного с показателями здоровья пользователей. В связи с этим многие онлайн-разработчики внедряют функции ограничения воздействия контента или поощрения активных перерывов.

Так, британская некоммерческая благотворительная организация SWGfl, продвигающая позитивные политики использования Интернета, отмечает, что на цифровое благополучие детей могут влиять следующие факторы:

— чрезмерная зависимость от технологий;

— подверженность цифровым рискам;

— отсутствие разумного баланса между онлайн- и офлайн-жизнью;

— негативное социальное интернет-взаимодействие.

Кроме того, в рамках рассматриваемого вопроса необходимо обратить внимание на материал об онлайн-безопасности платформы для развития движения за цифровые права в Азиатско-Тихоокеанском регионе Coconet, в котором она предложила несколько практик для поддержания цифровой гигиены:

— создание надежных паролей;

— регулярное обновление онлайн-инструментов;

— хранение резервных копий персональных файлов;

— защита подключения к Интернету;

— использование безопасных браузеров и HTTPS-соединений;

— знания о фишинговых атаках;

— информированность о возможностях сквозного шифрования;

— практика цифрового детокса.

РОЛЬ ОНЛАЙН-ПЛАТФОРМ И ЦИФРОВЫХ СЕРВИСОВ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ДЕТЕЙ В ИНТЕРНЕТЕ

ЗНАЧИМЫЕ КЕЙСЫ ОНЛАЙН-ПЛАТФОРМ И ЦИФРОВЫХ СЕРВИСОВ

В условиях нарастающих рисков для детей в Сети, реагируя на запрос общественного мнения, интернет-платформы принимают меры по повышению уровня онлайн-безопасности несовершеннолетних.

Так, в 2021 году видеохостинг YouTube отключил функцию автовоспроизведения роликов, а также внедрил напоминания «сделать перерыв» и «перед сном» для лиц младше 18 лет. Первое блокирует экран устройства спустя установленное количество времени, предлагая передохнуть от просмотра.

Второе при заранее включенном таймере напоминает о наступлении ночи и советует перенести видеосеанс на следующий день.

Социальная сеть Instagram тоже представила полезную функцию — запрет для взрослых на отправку сообщений детям, не подписанным на них. При этом сервис TikTok решил не отсылать несовершеннолетним push-уведомления в вечернее и ночное время.

Кроме того, для защиты детей в Интернете все больше онлайн-разработчиков прибегают к серьезным процедурам проверки возраста пользователей. Однако многие из них до сих пор игнорируют такие действия. Согласно исследованию ирландской организации CyberSafeKids, поднимающей вопросы онлайн-безопасности, 82 % детей от 8 до 12 лет зарегистрированы в соцсетях и пользуются приложениями для обмена сообщениями. Данный факт вызывает интерес в связи с тем, что, как правило, цифровые платформы официально запрещают лицам младше 13 лет пользоваться своими услугами, тем не менее без должной реакции осознают наличие таковых в числе своей аудитории.

Например, TikTok в 2019 году был оштрафован Федеральной торговой комиссией США на 5,7 миллиона долларов за нарушение COPPA. В деле указывалось, что компания обладала информацией об использовании ее платформы детьми, но не запрашивала на это согласия их родителей.

Еще один риск для цифровой безопасности несовершеннолетних — их склонность к участию в различных онлайн-испытаниях без прогноза последствий. В связи с этим британская радиовещательная корпорация BBC создала видеоклип для обсуждения этой проблемы с детьми. В нем трое блогеров, участвовавших в онлайн-испытаниях против боли, столкнулись лицом к лицу с матерью, ребенок которой погиб в результате одного из таковых. Ролик стал убедительным доказательством потенциальных рисков подобных занятий, а также раскрыл корыстные мотивы блогеров, продвигающих их.

Стоит также отметить, что в приложении № 3 обзора представлен список более безопасных альтернатив обычным инструментам для обеспечения цифровой гигиены.

GOOGLE

Американская транснациональная корпорация Google реализует программу обучения детей безопасности в Сети Be Internet Awesome, в рамках которой предоставляет информацию об основах цифровой гражданственности.

Инициатива Future of the Classroom нацелена на информирование сектора образования о необходимости совершенствовать технологическое оснащение учебных заведений, а также о современных вызовах, к которым следует адаптировать школьные программы.

Приложение видеохостинга YouTube Kids фильтрует контент в соответствии с возрастом и позволяет родителям следить за тем, что смотрят их дети.

Детское виртуальное пространство Kids Space, встроенное в качестве дополнительной «операционной системы» в некоторые мобильные устройства, включает в себя все основные функции смартфона, но предлагает ребенку только тщательно отобранные приложения, игры, книги и мультфильмы.

Вкладка «Дети» в магазине приложений Play представляет подборку одобренных учителями онлайн-товаров.

Семейная служба родительского контроля Family Link позволяет ограничивать контент, экранное время и тому подобное для контролируемых устройств детей.

Инструмент Digital Wellbeing дает возможность контролировать умные колонки и дис-

плеи: ограничивать контент и проставлять таймеры отключения. Также вскоре будут запущены новые фильтры для блокировки нежелательных новостей и подкастов.

К полезному опыту корпорации Google — только уже не с точки зрения повторения, а с точки зрения недопущения подобного — также можно отнести ее неоднократное включение в список «Грязная дюжина» Национального центра сексуальной эксплуатации США. Кампания была создана для побуждения гигантов цифровой отрасли содействовать в борьбе с насилием и эксплуатацией в Сети.

После включения в списки Google повысила безопасность компьютеров нового типа Chromebook для учащихся, установила правила удаления из Play приложений, пропагандирующих «вознаграждаемые сексуальные отношения», в сервисе контекстной рекламы Ads отказалась от рекламы порнографического содержания и расширила инструменты фильтрации Wi-Fi. Однако в 2022 году компанию снова причислили к «Грязной дюжине». На этот раз составители списка затребовали от Google тщательнее поработать над политикой и практикой борьбы с сексуальным насилием в Интернете, заявив, что «с большими возможностями приходит и большая ответственность».

ESET

В апреле 2022 года международный разработчик антивирусного программного обеспечения и решений в области компьютерной безопасности ESET запустил платформу Safer Kids Online, посвященную созданию защищенной онлайн-среды для несовершеннолетних. На ней представлены как тематическая экспертная информация и викторины для родителей и учителей, так и обучающие мультфильмы и комиксы для детей разного возраста. Рекомендации о безопасности в Сети составлены детскими психологами и экспертами по кибербезопасности. В них можно найти советы о том, как управлять экранным временем, отслеживать признаки кибербуллинга или ограждать детей от онлайн-хищников.

Кроме того, Safer Kids Online предоставляет бесплатное приложение для родительского контроля — ESET Parental Control для Android. Оно позволяет управлять онлайн-временем детей и фильтровать просматриваемый ими контент.

В будущем ESET планирует реализовать инициативы по обеспечению безопасности несовершеннолетних в Интернете по всему миру — от Европы и Азии до США и Латинской Америки — в сотрудничестве с местными партнерами и неправительственными организациями. Разработчик уже начал такое взаимодействие с Великобританией — ESET UK и неправительственной организацией по безопасности детей Internet Matters.

TIKTOK

За последние несколько лет сервис для создания и просмотра коротких видео TikTok не раз подвергался критике и, как и Google, в 2020 году был включен в список «Грязная дюжина» Национального центра сексуальной эксплуатации США за то, что стал «излюбленной платформой для онлайн-хищников». Также инициатива обвинила TikTok в том, что из-за него, по данным Министерства внутренней безопасности США, с 2019 по 2021 год количество расследований эксплуатации детей увеличилось в семь раз.

При этом составители списка отметили, что в итоге руководство соцсети услышало призывы и предприняло ряд мер:

— отключило прямой обмен сообщениями для лиц младше 16 лет;

— разрешило родителям блокировать элементы управления с помощью ПИН-кода;

— выпустило обширные Принципы сообщества, четко определяющие термины и перечисляющие действия и контент, запрещенные на платформе, включая контент, который «изображает, пропагандирует или прославляет» проституцию или порнографию, контент, имитирующий сексуальную активность или секс без согласия.

Примечательно, что TikTok достойно принимает недовольства общественности и достаточно оперативно реагирует на них. В частности, компания создала Руководство для ответственных за воспитание детей. В нем представлено множество инструментов продукта и элементов управления им для обеспечения безопасности несовершеннолетних. Также в руководстве содержится общая информация о распространенных онлайн-рисках.

Кроме того, TikTok ужесточил политику в отношении вредоносного контента. Среди нововведений такого порядка — функция «фильтровать комментарии». При ее активации мнения аудитории о том или ином видео перед публикацией отправляются непосредственно создателю контента. Он, в свою очередь, самостоятельно решает, отсылать комментарии на просторы Сети или нет.

FACEBOOK

Как свидетельствуют данные сервиса CyberTipline Национального центра пропавших без вести и эксплуатируемых детей США, в 2020 году подавляющее большинство онлайн-сообщений о сексуальном насилии над несовершеннолетними и торговле ими фиксировалось в крупнейшей социальной сети мира Facebook. На нее пришлось почти 95 % текстовых отправлений из 21,7 миллиона отчетов всех платформ.

Как следует из данных ресурса Internet Safety 101, правоохранительные органы все чаще сталкиваются с проблемой, когда из-за онлайн-продуктов с шифрованием интернет-сообщение видит только конечный пользователь. В связи с этим не хватает доказательств для начала судебного преследования, даже когда дело касается национальной безопасности. Шифрование за счет анонимности облегчает осуществление злодеяний террористам и другим преступникам.

В связи с этим в октябре 2019 года американское Министерство юстиции опубликовало открытое письмо к соцсети Facebook от лидеров США, Великобритании и Австралии в ответ на публичные заявления компании о внедрении сквозного шифрования в ее сервисы обмена сообщениями.

При этом также интересен тот факт, что, несмотря на заявления Facebook о повышенном внимании к политике онлайн-безопасности, в Великобритании звучат мнения о том, что компания предоставляет ложную картину усилий по борьбе с ненавистническими высказываниями и другим неблагоприятным контентом.

INSTAGRAM

Американская социальная сеть Instagram опубликовала руководство для родителей, призванное помочь безопасному пребыванию детей на платформе. В него включен обзор ряда тематических функций и элементов, среди которых:

— управление комментариями;

— ограничение прямых сообщений между незнакомыми детьми и взрослыми;

— блокировка нежелательных контактов и жалобы на них;

— отслеживание попыток подозрительного взаимодействия с ребенком.

Отдельно стоит отметить еще одну новую функцию Instagram. Ее задача заключается в выделении оскорбительных слов при их наборе пользователем и отправке ему уточняющего вопроса о степени его уверенности в своих действиях. Примечательно, что аналитики фиксируют довольно высокий показатель успеха нововведения: обидные сообщения после предупреждения отправляются менее чем в 50 % случаев.

Однако Instagram все-таки наносит вред значительному проценту детей, особенно девочкам-подросткам. Например, как отмечается в статье The New York Times, в США компания сталкивается с расследованиями влияния соцсети на психическое здоровье подростков.

MOZILLA

Некоммерческая организация Mozilla в целях обеспечения справедливого доступа к Интернету всех людей планеты разработала карту основных навыков веб-грамотности. Специалисты уверены, что в XXI веке к базовым умениям — чтению, письму и арифметике, необходимым для достижения успеха в современном мире, добавился навык работы с цифровой средой.

При этом на ресурсе не только даны общие сведения о сферах повышения цифровой грамотности, но и представлены конкретные навыки для каждой компетенции. Кроме того, они сопровождены описанием определенных действий, которые необходимо предпринять для овладения ими.

ПОДОТЧЕТНОСТЬ И ОБЩЕСТВЕННЫЙ МОНИТОРИНГ ОНЛАЙН-ПЛАТФОРМ И ЦИФРОВЫХ СЕРВИСОВ

Национальный центр пропавших без вести и эксплуатируемых детей США посредством системы CyberTipline получает сообщения о случаях сексуального надругательства над детьми в Интернете, анализирует их, а затем предоставляет в виде ежегодной отчетности (таблица № 2). Также специалисты центра передают полученные сведения о CSAM правоохранительным органам для дальнейшего расследования.

Кроме того, Национальный центр пропавших без вести и эксплуатируемых детей США составил Руководство по удалению из Интернета обнаженных или сексуально-эксплуатационных материалов с несовершеннолетними. В нем содержится как информация о системе CyberTipline, так и рекомендации взаимодействия по данному вопросу с другими ресурсами.

Шведская компания NetClean позиционирует себя как мирового лидера в области технических решений, призванных остановить распространение материалов о жестоком обращении с детьми в Интернете.

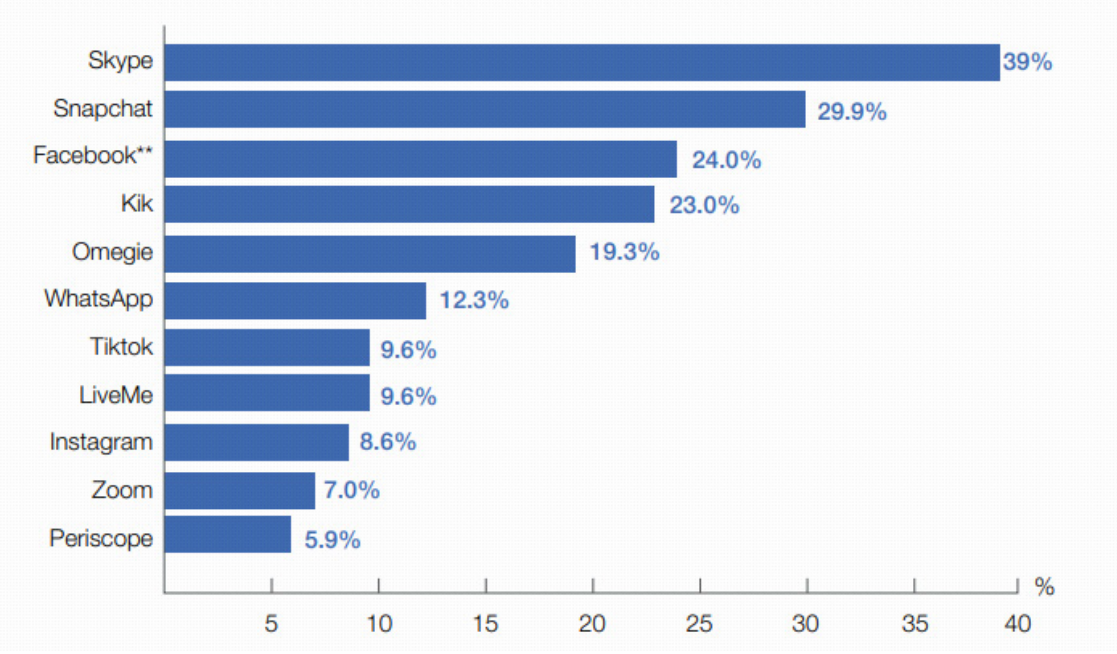
Она разрабатывает программные обеспечения для обнаружения и блокировки файлов с сексуальным насилием над несовершеннолетними на рабочих ИТ-устройствах с целью защиты предприятий, повышения их устойчивости и снижения реального вреда детям.

Кроме того, каждый год NetClean публикует признанный на международном уровне отчет, в котором освещаются различные аспекты борьбы с сексуальным насилием над детьми в Интернете. Так, в документе за 2019 год было выявлено, что распространение CSAM растет, несмотря на международный консенсус о незаконности таких материалов. Особенно для популяризации такого контента используются прямые трансляции (рисунок № 4).

Таблица № 2. Количество сообщений по каждому типу инцидентов

КАТЕГОРИЯ ОТЧЕТНОСТИ	2019	2020	2021
CSAM: владение, производство и распространение	16 939 877	21 669 264	29 309 106
Детский секс-туризм	683	955	1624
Торговля несовершеннолетними в целях сексуальной эксплуатации	11 798	15 879	16 032
Сексуальные домогательства к детям	4747	11 770	12 458
Вводящее в заблуждение доменное имя	838	3109	3304
Вводящие в заблуждение слова или цифровые изображения	8631	8689	5825
Онлайн-соблазнение детей на реальные половые акты	19 174	37 872	44 155
Непристойные материалы, отправленные несовершеннолетним без их запроса	1613	3547	5177
Общий итог	16 987 361	21 751 085	29 397 681

Рисунок № 4. Процент назвавших конкретные ресурсы с трансляциями сексуального наслия над детьми в прямом эфире



Источник: NetClean

ИТОГОВЫЕ ВЫВОДЫ В РАМКАХ РАССМОТРЕННОГО МЕЖДУНАРОДНОГО ОПЫТА

Защита детей в Интернете является важной социальной задачей, которая требует вовлеченности всех акторов и системного подхода. Проблемы несовершеннолетних в онлайн-среде так же реальны и ощутимы, как в физическом мире. Дети весьма значительную часть времени уделяют общению, играм, обмену музыкой и фильмами, изучению учебного материала с использованием онлайн-инструментов. Поэтому необходимо обеспечить их права в цифровой среде, гарантированные лучшими стандартами, используя эффективные правовые, институциональные и технологические механизмы.

Анализ зарубежных подходов и практик по вопросам обеспечения защиты детей в онлайн-пространстве, включая меры повышения цифровой грамотности, показывает, что ключевая роль в обеспечении безопасности несовершеннолетних в цифровой среде отводится родителям и преподавателям. При этом сложность вызывает то обстоятельство, что цифровая грамотность у них зачастую не соответствует требуемому уровню знаний для обеспечения такой защиты: не всегда используются выверенные методики коммуникации с ребенком, недостаточно технических знаний и информации о том, куда можно обратиться за помощью и где получить квалифицированную консультацию.

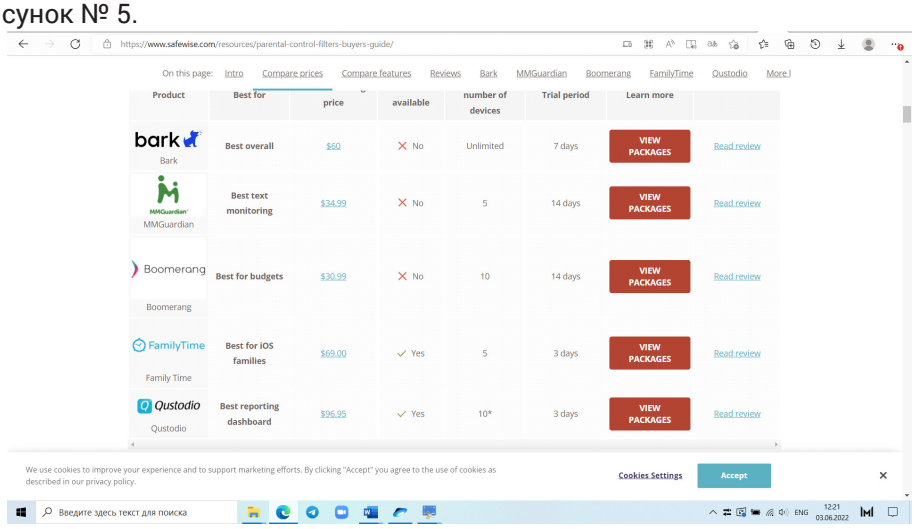
На международном уровне все еще ощущается недостаток скоординированной работы, которая была бы сосредоточена на безопасности детей в Интернете. Отсутствие комплексных законодательных мер как на глобальном уровне, так и в рамках отдельных юрисдикций привело к внедрению целого ряда продуктов и услуг, которые главным образом ориентированы на получение прибыли. Процесс действенного саморегулирования технологических компаний продвигается достаточно медленно и в некоторых случаях явно отстает от реалий сегодняшнего дня. Нередко платформы и соцсети перекладывают ответственность на родителей, педагогов, образовательные учреждения, да и на самих детей, которые в силу понятных причин не могут обеспечить свою безопасность в столь противоречивом, постоянно меняющемся мире.

Отдельно стоит отметить, что значительная часть различных практических методик, которые разрабатываются для родителей, распространяется на платной основе.

Так, стоимость программ, входящих в топ-10 для родительского контроля, варьируется от 30 до 97 долларов США в год.

Для многодетных семей и родителей в развивающихся странах оплата таких продуктов затруднительна. Ниже приведены данные о стоимости некоторых программ родительского контроля (рисунок № 5):В основе тенденций в области обеспечения безопасности детей в Интернете лежат документы ООН, которые задают вектор разра-

Рисунок № 5.



Источник: SafeWise

ботки и внедрения различных инструментов.

Политики, регуляторы и общественные организации стремятся к тому, чтобы росла осведомленность детей о существующих в Сети рисках. Параллельно с этим самостоятельное критическое мышление ребенка приобретает все большее значение. Становится очевидным, что необходимо развивать у детей навыки, которые позволят им самостоятельно правильно распознать и оценить риски и угрозы их безопасности. При этом важно создать условия, чтобы дети не боялись обращаться за помощью и консультацией к специалистам, педагогам или родителям. В изученных документах прослеживается тенденция, что такого рода навыки формируются сейчас по четырем направлениям:

— в рамках школьных программ;

— за счет повышения ответственности родителей;

— за счет практических мер и инструментов частного бизнеса и цифровых платформ;

— посредством распространения в детской и родительской средах лучших практик силами государства, а также правозащитными и общественными организациями и добровольными объединениями.

Важно, чтобы несовершеннолетние в Интернете могли идентифицировать опасность: фейки, кибербуллинг, материалы о сексуальном насилии над несовершеннолетними или различные признаки сексуализации и соблазнения, риски утечки личной информации и другие. Обнаружив такие опасности или испытывая сомнения в отношении каких-либо событий или контента в Сети, дети и их родители должны знать, куда им можно обратиться за помощью.

Такие возможности должны быть предоставлены в том числе за счет организации горячих линий, которые вызывали бы доверие и имели хорошую репутацию у детей и родителей.

По мнению экспертов, некоторые платформы не в состоянии гарантировать безопасность ребенка, поэтому в настоящее время наблюдаются тенденции, когда родители вынуждены нести на себе значительную долю ответственности за безопасность детей.

В этих условиях родителям необходимо:

— быть осведомленными о рисках и проблемах Интернета, чтобы на безопасной основе использовать его в семье;

— поддерживать с детьми доверительный диалог;

— устанавливать на домашние компьютеры программное обеспечение, которое может отслеживать и блокировать негативные, вредные или явно опасные материалы.

Повышение цифровой грамотности родителей в Интернете — важная составляющая в деле защиты детей. Необходимо проводить семинары, консультации, развивать эффективные методики выявления угроз, осуществлять другие мероприятия,которыебудутспособствоватьлучшему пониманию взглядов детей и той среды, в которой происходит формирование их личностей.

Исследование «Общая ответственность: обеспечение устойчивости детей в Интернете», проведенное Оксфордским институтом Интернета совместно с экспертной консалтинговой компанией в области цифровой семейной жизни ParentZone в 2014 году, показало, что поддержка родителей сыграла ключевую роль в том, чтобы дети научились справляться с проблемами в эпоху онлайн-технологий. А развитие цифровых навыков и способность разрабатывать стратегии в онлайн-мире так же, как и в реальной жизни, — это ключи к повышению устойчивости и самостоятельности молодежи.

Было выявлено, что родительские стратегии ограничения и контроля могут быть полезны для прямой защиты детей от потенциального вреда. Вместе с тем некоторые жесткие запреты старших имели непреднамеренные негативные последствия, подрывали психологическую устойчивость детей и их конструктивную активность в Интернете. Воздействие на детей со стороны взрослых, их воспитание и опека в вопросах онлайн активности – сложный процесс, где ключевыми факторами являются доверие, атмосфера сотрудничества и взаимопонимания.

Следует особо подчеркнуть, что позиция по возложению всей ответственности на родителей может привести к искаженному пониманию проблемы. Цифровая среда не должна быть подобна водоему с хищниками, где каждый спасается, как может. Бизнес должен стремиться предпринять все возможные технические и организационные меры, чтобы снизить риски для детей, своевременно выявлять и устранять новые угрозы и опасные практики, которыми пользуются преступники. Также имеет значение и просветительская роль бизнеса, максимально прозрачное информирование о зонах потенциального риска, внедрение бес-

платных и надежных инструментов защиты и доведение до населения таких возможностей.

По мнению экспертов блога LSE Лондонской школы экономики о воспитании детей в цифровом мире, для того чтобы повысить уровень онлайн-медиаграмотности, следует:

— проводить оценку реализуемых практик и инициатив;

— осуществлять финансирование долгосрочных программ для устойчивых изменений;

— усиливать координацию национальных организаций, занимающихся вопросами цифрового образования;

— ликвидировать разрыв между реальным обучением и формальными школьными программами и образовательными структурами, наладить взаимодействие между школьным и внешкольным обучениями;

— отказаться от устаревших методов оценки измерения медиаграмотности, применять не универсальные подходы, а адаптированные для различных групп детей;

— нарастить исследовательскую базу для понимания реальных проблем и принятия наиболее эффективных решений, активнее применять статистические данные, анкетирование детей, родителей и педагогов.

Приведенные в обзоре практики, инструментарий и зарубежный опыт требуют тщательного анализа и осмысления применительно к российской среде. Вероятно даже самые эффективные меры, реализованные за рубежом, в случае применения их в России должны быть адаптированы и пройти серьезное экспертное заключение. Все практические методики, безусловно, должны учитывать национальную и региональную специфику, культурные ценности и традиции, особенности рынка услуг, поведенческие характеристики детской аудитории по возрастным группам.

Реализация политики по защите детей в онлайн-пространстве может иметь положительный эффект только при заинтересованном и ответственном участии всех акторов, прежде всего регуляторов, надзорных органов, бизнеса, образовательных и воспитательных учреждений, родителей, общественных организаций. Немаловажной представляется работа по сбору статистики и проведению других измерений, которые должны стать основой для всестороннего, прежде всего научного анализа, с целью выявления насущных проблем и поиска их решений. Необходимо поднять на новый уровень работу статистических служб и исследовательских команд, интенсифицировать кампании по опросу и анкетированию, эффективнее накапливать и тщательно взвешивать информацию из образовательных учреждений и домохозяйств.

В современном, быстроменяющемся мире важно правильно расставить приоритеты, имея в виду риск-ориентированный подход, продуманную последовательность шагов в зависимости от возникающих угроз и оценки потенциального ущерба.

Целесообразно выстраивать работу на опережение и предупреждение, уделять внимание профилактике и устранению рисков на этапе их раннего выявления. В этих целях следует модернизировать методики и инструменты сбора и интерпретации полезных данных, выявлять новые аспекты и критерии, которые подлежат анализу в рамках рассматриваемой проблемы.

Для эффективной профилактики, контроля и реагирования необходимо сосредоточить усилия по налаживанию и поддержанию заинтересованного и конструктивного межинституционального диалога, укреплять связи между профильными организациями, поощрять и использовать прогрессивные инициативы и новации.

ПРИЛОЖЕНИЕ № 1

ПЕРЕЧЕНЬ И КРАТКОЕ ОПИСАНИЕ ДОПОЛНИТЕЛЬНЫХ ЗАРУБЕЖНЫХ ИНИЦИАТИВ И ИНСТРУМЕНТОВ В СФЕРЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДЕТЕЙ В ЦИФРОВОЙ СРЕДЕ, КОТОРЫЕ ПОДРОБНО НЕ РАССМАТРИВАЮТСЯ В ОСНОВНЫХ РАЗДЕЛАХ ОБЗОРА

5RIGHTS FOUNDATION

Международная неправительственная некоммерческая благотворительная организация работает над продвижением цифровых прав детей. В настоящий момент занимается созданием Справочника по глобальной политике защиты несовершеннолетних в Интернете

360SAFE

Инструмент самопроверки для пересмотра образовательными учреждениями политики безопасности в Сети

CHILDNET

Британская благотворительная организация занимается сбором реального онлайн-опыта детей, родителей и учителей, а также предоставляет им бесплатные ресурсы о цифровом благополучии

CYBERANGELS

Американское виртуальное образовательное сообщество обучает безопасности в Интернете. На его портале советам по защите детей в Сети посвящен целый раздел

ENACSO

Европейский альянс неправительственных организаций, финансируемый Еврокомиссией, работает над созданием безопасной онлайн-среды для несовершеннолетних посредством информационно-пропагандистских мероприятий на национальном, европейском и международном уровнях. В 2014 году разработал проект программного документа «Бизнес, дети и Интернет: когда бесплатность — это не так», в котором содержится подробный анализ ориентированности различных бизнес-моделей в Сети на несовершеннолетних, а также анализ нарушений ими Конвенции ООН по правам ребенка

REPORTBULLYING

Американская компания предлагает комплексные программы по борьбе с травлей детей, предоставляет спикеров по этой тематике и руководит работой приложения, позволяющего отправлять анонимные сообщения о кибербуллинге непосредственно администрации учебного заведения

INTERNET MATTERS

Британская неправительственная организация по безопасности детей в цифровой среде занимается информированием, поддержкой и поиском инструментов в рамках данной тематики. Так, на ее портале найдутся различные исследования и универсальный ресурсный центр с руководствами для родителей и учителей

FAMILY ONLINE SAFETY INSTITUTE

Международная некоммерческая организация работает над созданием более безопасного для семей онлайн-мира и внедрением цифровой гражданственности, объединяя лидеров отрасли, правительства и представителей некоммерческого сектора

GLOBAL KIDS ONLINE

Международный исследовательский проект нацелен на создание и поддержание межнациональной базы фактических данных об использовании Интернета детьми путем создания глобальной сети исследователей и экспертов. В рамках проекта разработан глобальный исследовательский инструментарий, который позволяет ученым, правительствам, гражданскому обществу и другим субъектам проводить надежные и стандартизированные исследования с участием детей и их родителей о возможностях, рисках и защитных факторах, связанных с использованием Интернета несовершеннолетними

TENCENT

Китайская компания Tencent позиционирует себя как ведущую мировую интернет- и технологическую организацию и разрабатывает инновационные продукты и услуги для улучшения качества жизни. Реализует проект Humiao — онлайн- и офлайн-курсы для несовершеннолетних, родителей и учителей о цифровой грамотности и онлайн-самозащите

YOUTHFORESIGHT

Глобальная платформа содержит инструменты, экспертные статьи, интерактивные материалы, базы данных для реализации действий по улучшению образования, навыков и занятости молодых людей. Также на ней функционирует форум для обсуждения позитивных изменений в жизни молодежи

CHILDHOOD

Международный фонд инвестирует в создание эффективных цифровых решений для безопасности детей в Сети, а также поддерживает инновационные онлайн-службы помощи и новаторские технологии для выявления CSAM

ПРИЛОЖЕНИЕ № 2

НЕКОТОРЫЕ НАИБОЛЕЕ ПОПУЛЯРНЫЕ ИНТЕРНЕТ-РЕСУРСЫ ДЛЯ ДЕТСКОЙ АУДИТОРИИ

AMINO

общение по интересам текстом, голосом или посредством общего просмотра видео в чате.

СОЦИАЛЬНАЯ СЕТЬ ASKFM

анонимные и персонализированные вопросы интересующим людям.

CALCULATOR VAULT

сокрытие фото, видео и других приложений.

САЙТЫ CHATROULETTE

общение посредством текста или видео с пользователями, случайно выбранными системой.

МЕССЕНДЖЕР DISCORD

поддерживает телефонную связь и видеоконференции, часто используется геймерами и студентами.

FACEBOOK

одна из крупнейших социальных сетей в мире.

ПЛАТФОРМА FACEBOOK LIVE

общение в прямом эфире.

ПРИЛОЖЕНИЕ FACEBOOK MESSENGER KIDS

обмен сообщениями среди детей.

ПРИЛОЖЕНИЕ HOUSEPARTY

организация групповых видеочатов.

СОЦИАЛЬНАЯ СЕТЬ INSTAGRAM

обмен фото, видео и аудио, чтение материалов блогеров на интересующие темы.

ПРИЛОЖЕНИЕ KIK

мгновенный обмен сообщениями.

ПРИЛОЖЕНИЯ LINE

аудио- и видеозвонки, обмен текстом и файлами.

СОЦИАЛЬНАЯ СЕТЬ LIVEME

ведение и просмотр прямых трансляций.

СОЦИАЛЬНАЯ СЕТЬ MEETME

знакомства на основе географической близости.

ВЕБ-СЕРВИС OMEGLE

общение с незнакомцами один на один в анонимных чатах.

САЙТ REDDIT

социальная сеть и форум для обсуждения актуальных новостей и голосований.

ПЛАТФОРМА ROBLOX

участие в многопользовательских играх, их создание
и личное и групповое общение.

СОЦИАЛЬНАЯ СЕТЬ SARAHAH

анонимные отзывы о знакомых и случайных людях.

ПРИЛОЖЕНИЕ SNAPCHAT

обмен фото и видео, которые удаляются спустя определенное время.

МЕССЕНДЖЕР TELEGRAM

обмен текстовыми сообщениями, фото, видео и файлами, а также совершение телефонных звонков.

СЕРВИС TIKTOK

создание и просмотр коротких видео.

СЛУЖБА МИКРОБЛОГОВ TUMBLR

публикация и чтение текстовых

и медиаматериалов с разной тематикой.

СЕРВИС TWITCH

прямые трансляции для геймеров.

СЕРВИС МИКРОБЛОГОВ TWITTER

отправка, чтения и комментирование коротких сообщений.

ПРИЛОЖЕНИЕ VSCO

съемка и обработка фотографий.

МЕССЕНДЖЕР WECHAT

передача текстовых и голосовых сообщений.

СЕРВИС WHATSAPP

обмен мгновенными текстовыми и медиасообщениями, телефонные звонки.

СОЦИАЛЬНАЯ СЕТЬ WHISPER

анонимный обмен мыслями, новостями, фото и видео.

ВИДЕОХОСТИНГ YOUTUBE

хранение, публикация и просмотр роликов.

ПРИЛОЖЕНИЕ YUBO

знакомства с новыми людьми для подростков.

СЛУЖБА ВЕЩАНИЯ YOUNOW

организация или просмотр прямых трансляций.

ПРИЛОЖЕНИЕ № 3

СПИСОК НЕКОТОРЫХ ИНСТРУМЕНТОВ ДЛЯ ОБЕСПЕЧЕНИЯ ЦИФРОВОЙ ГИГИЕНЫ

МЕНЕДЖЕРЫ ПАРОЛЕЙ

KeePassXC

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ ШИФРОВАНИЯ ФАЙЛОВ ПЕРЕД СОХРАНЕНИЕМ

Cryptomator

БЕСПЛАТНЫЕ VPN

RiseupVPN, ProtonVPN, TunnelBear

БРАУЗЕРЫ И HTTPS-СОЕДИНЕНИЯ

Brave, Firefox, Chromium

ПОИСКОВАЯ СИСТЕМА

DuckDuckGo

РАСШИРЕНИЯ БЕЗОПАСНОСТИ БРАУЗЕРА

HTTPS Everywhere, Privacy Badger, NoScript, uBlock Origin

БЕСПЛАТНЫЙ АНАЛИТИК ФАЙЛОВ И URL-АДРЕСОВ НА НАЛИЧИЕ ВРЕДОНОСНОГО КОНТЕНТА

VirusTotal

СОВМЕСТНАЯ РАБОТА НАД ДОКУМЕНТАМИ

CryptPad, Riseup Pads

ЧАТ-ПРИЛОЖЕНИЯ

Signal, Wire, Rocket

ПОЧТОВЫЕ СЕРВИСЫ

Protonmail, Tutanota

ПЛАТФОРМЫ ДЛЯ ВИДЕОКОНФЕРЕНЦИЙ

Jitsi, Talky, Wire, Mumble

КОРПОРАТИВНЫЕ ОБЛАЧНЫЕ ХРАНИЛИЩА ДЛЯ ОБМЕНА ФАЙЛАМИ

ShareRiseup, OnionShare

СПИСОК ДОПОЛНИТЕЛЬНЫХ ИСТОЧНИКОВ, ИСПОЛЬЗОВАННЫХ ПРИ ПОДГОТОВКЕ ОБЗОРА

A. Hidayati, R. Efendi, A. Saputra / «The Quality of Digital Literation Early Childhood: Education Teachers Based on UNESCO Standards» // International Journal of Scientific & Technology Research. — March 2020. — https://www.ijstr.org/final-print/mar2020/The-Quality-Of-Digital-Literation-Early-Childhood-Education-Teachers-Based-On-Unesco-Standards.pdf.

A. Katz, A. El Asam / «The Cybersurvey. In Their Own Words: The Digital Lives of Schoolchildren» // Internet Matters. — 2020. — https://www.internetmatters.org/wp-content/uploads/2020/10/Internet-Matters-CyberSurvey19-Digital-Life-Web.pdf.

A. D. Yazon, K. Manaig, C. A. C. Buama, J. F. B. Tesoro / Digital Literacy, Digital Competence and Research Productivity of Educators // Universal Journal of Educational Research. — August 2019. — https://www.researchgate.net/publication/335300170_Digital_Literacy_Digital_Competence_and_Research_Productivity_of_Educators.

T. Burns, F. Gottschalk / «Educating 21st Century Children: Emotional Well-being in the Digital Age» // Educational Research and Innovation. — October 2019. — https://doi.org/10.1787/b7f33425-en.

I. Clifford, S. Kluzer, S. Troia, M. Jakobsone, U. Zandbergs / DigCompSAT // Publications Office of the European Union. — 2020. — https://all-digital.org/wp-content/uploads/2021/01/digcompsat_2020.pdf.

E. Englander, E. Donnerstein, R. Kowalski, C. A Lin, K. Parti / Defining Cyberbullying // Pediatrics. — November 2017. — https://pubmed.ncbi.nlm.nih.gov/29093051/.

J. Hanley / Establishing a Family Online Safety Contract // Family Online Safety Institute. — February 2017. — https://www.fosi.org/good-digital-parenting/establishing-family-online-safety-contract.

H. Zapal / 2018 Children & Teen Cyber Fact Sheet // The Bark Blog. — January 2019. — https://www.bark.us/blog/2018-children-and-teen-cyber-fact-sheet/.

«The Global Partnership to End Violence Against Children: Partnership Strategy 2022–2024» // End Violence Against Children. — https://www.end-violence.org/sites/default/files/2022-04/End%20Violence%20Partnership%20Strategy%202022-24%20%281%29.pdf.

«Kids & Tech: The Evolution of Today's Digital Natives» // Influence Central. — 2016. — https://influence-central.com/trendspotting/kids-tech-the-evolution-of-todays-digital-natives/.

Guidelines for Industry on Child Online Protection // International Telecommunication Union. — June 2020. — https://www.itu.int/en/mediacentre/Pages/pr10-2020-Guidelines-Child-Online-Protecion.aspx.

Guidelines on Child Online Protection // International Telecommunication Union. — 2020. — https://www.itu-cop-guidelines.com/.

J. W. Patchin / 2019 Cyberbullying Data // Cyberbullying Research Center. — July 2019. — https://cyberbullying.org/2019-cyberbullying-data.

K. Muir, A. Joinson / An Exploratory Study into the Negotiation of Cyber-Security Within the Family Home // Frontiers in Psychology. — March 2020. — https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7081791/.

L. Levi / Media Literacy Beyond the National Security Frame // University of Miami School of Law Institutional Repository. — 2020. — https://repository.law.miami.edu/fac_articles/927/.

L. M. Jones, K. J. Mitchell / Defining and Measuring Youth Digital Citizenship // New Media & Society. — March 2015. — https://journals.sagepub.com/doi/abs/10.1177/1461444815577797.

«The Online Enticement of Children: An In-Depth Analysis of CyberTipline Reports» // National Center for Missing and Exploited Children. — 2017. — https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/Online%20Enticement%20Pre-Travel.pdf/.

«Internet Safety: Children 6–8 Years» // Raising Children Network. — 2021. — https://raisingchildren.net.au/school-age/safety/online-safety/internet-safety-6-8-years.

R. Efendi, J. Jama, A. Yulastri / Development of Competency Based Learning Model in Learning Computer Networks // «Journal of Physics: Conference Series». — March 2019. — https://iopscience.iop.org/article/10.1088/1742-6596/1387/1/012109/pdf.

Cyber Safety Consideration for K-12 Schools and School District // Readiness and Emergency Management for Schools // Technical Assistance Center. — 2020. — https://rems.ed.gov/docs/Cyber_Safety_K-12_Fact_Sheet_508C.PDF.

Report of a National Survey of Children, Their

Parents and Adults Regarding Online Safety // Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media. — November 2021. — https://www.gov.ie/en/publication/1f19b-report-of-a-national-survey-of-children-their-parents-and-adults-regarding-online-safety/.

R. Rodrigues / What is Digital Hygiene? // Digital Hygiene. — November 2014. — http://digitalhygiene.com/2010/11/04/what-is-digital-hygiene/.

E. Staksrud, S. Livingstone / «Children and Online Risk: Powerless Victims or Resourceful Participants?» // Information, Communication & Society. — 2009. — https://www.tandfonline.com/doi/abs/10.1080/13691180802635455.

D. Kuzmanovi , Z. Pavlovi , D. Popadi , T. Milosevic / «Internet and Digital Technology: Use among Children and Youth in Serbia» // EU Kids Online. — 2018. — https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/participant-countries/serbia/EU-Kids-Online-ENG-2019.pdf.

General comment no. 25 on Children's Rights in Relation to the Digital Environment — 2021. — https://5rightsfoundation.com/uploads/ExplanatoryNotes_UNCRCGC25.pdf.

«Information Society Policies. Annual World Report» // UNESCO. — 2009. — https://ifap.ru/library/book462.pdf.

ICT Competency Framework for Teachers // UNESCO. — 2018. — https://en.unesco.org/themes/ict-education/competency-framework-teachers.

«Children's Rights and the Internet: From Guidelines to Practice» // UNICEF — 2016. — https://www.unicef.org/csr/files/Childrens_Rights_and_the_Internet_Guidelines_to_Practice_Guardian_Sustainble_Business_English.pdf.

Children at Increased Risk of Harm Online during Global COVID-19 Pandemic // UNICEF in Turkey. — April 2020. — https://www.unicef.org/turkiye/en/press-releases/children-increased-risk-harm-online-during-global-covid-19-pandemic.

M. Brossard, M. Carnelli, S. Chaudron, R. Di-Gioia, T. Dreesen, D. Kardefelt-Winther, C. Little, J. L. Yameogo / «Digital Learning for Every Child: Closing the Gaps for an Inclusive and Prosperous Future» // Task Force 4 Digital Transformation. — September 2021. — https://www.unicef.org/media/113896/file/Digital%20Learning%20for%20Every%20Child.pdf.

F. Nascimbeni, S. Vosloo / «Scoping Paper. Digital Literacy for Children: Exploring Definitions and Frameworks» // UNICEF Office of Global Insight and Policy. — August 2019. — https://www.unicef.org/globalinsight/media/1271/file/%20UNICEF-Global-Insight-digital-literacy-scoping-paper-2020.pdf.

«More than 175,000 Children Go Online for the First Time Every Day, Tapping into Great Opportunities, but Facing Grave Risks» // UNICEF. — February 2018. — https://www.unicef.org/eca/press-releases/more-175000-children-go-online-first-time-every-day-tapping-great-opportunities.

S. Vandoninck, L. d'Haenens, R. de Cock, V. Donoso / Social Networking Sites and Contact Risks among Flemish Youth // Childhood. — August 2011. — https://doi.org/10.1177/0907568211406456.

L. Taddei / Impact of COVID-19 on Child Sexual Exploitation and Abuse Online // WeProtect Global Alliance. — May 2020. — https://www.weprotect.org/library/impact-of-covid-19-on-child-sexual-exploitation-online/.

F. Lalani, B. Mao / «Risks to Kids Online are Growing. Here's What We Can Do» // World Economic Forum. — October 2021. — https://www.weforum.org/agenda/2021/10/overcoming-the-growing-risks-to-kids-online.

G. P. Yustika, S. Iswati / «Digital Literacy in Formal Online Education: A Short Review» // Dinamika Pendidikan. — 2020. — https://journal.unnes.ac.id/nju/index.php/DP/article/view/23779/10468.