АЛЬЯНС
ПО ЗАЩИТЕ ДЕТЕЙ
В ЦИФРОВОЙ СРЕДЕ

Губернатору Приморского края
Кожемяко О.Н.

Уважаемый Олег Николаевич!

В рамках инициатив Альянса по защите детей в цифровой среде ПАО «Ростелеком» провел научное исследование «Технологии защиты детей в интернете». Результаты исследования могут применяться при разработке и совершенствовании технических мер защиты несовершеннолетних пользователей от киберугроз, а также в просветительской и образовательной деятельности.

В исследовании проанализированы 23 основных киберриска для детей и подростков, изучено более 300 патентов, компаний и ИТ-решений в сфере кибербезопасности, а также выявлены 10 областей, в которых с большой вероятностью будут формироваться угрозы в ближайшем будущем.

Из-за высокой степени опасности и недостаточности технических мер защиты в зону особого внимания отнесены разные виды психологического насилия над детьми в цифровой среде. Также выявлена недооценка рисков, связанных с маркетинговым и информационным давлением на ребенка. На основании результатов исследования Альянс по защите детей в цифровой среде сформировал рекомендации для органов государственной власти, образовательных учреждений, коммерческих предприятий, ИТ-разработчиков, родителей, НКО и социальных предпринимателей.

Просим Вас ознакомиться с исследованием для возможного использования в своей деятельности и тиражирования среди стейкхолдеров, заинтересованных в формировании защищенного и благоприятного для детей интернет-пространства.

С уважением,
председатель Альянса
по защите детей
в цифровой среде

Е.А. Белякова

АЛЬЯНС
ПО ЗАЩИТЕ ДЕТЕЙ
В ЦИФРОВОЙ СРЕДЕ

Технологии защиты детей в интернете

Ростелеком MINDSMITH TEQVISER

Новый цифровой мир помимо очевидных плюсов таит в себе немало опасностей, особенно для детей и подростков.

Исследование рисков, с которыми сталкиваются в сети несовершеннолетние, а также технологий их защиты как никогда актуально сейчас, в эпоху, когда весь мир перешел в онлайн. В силу возраста и отсутствия опыта дети особенно уязвимы для различного рода киберпреступников, поэтому мы должны уделять повышенное внимание их безопасности в интернете.

Кажется, что вопрос безопасности детей в интернете никогда не будет изучен до конца, ведь каждый год и даже каждый месяц мы наблюдаем появление новых угроз. Сегодняшние риски трансформируются, раскрываются и усиливаются под влиянием технологических трендов и глобальных изменений в обществе. Как мы можем обеспечить безопасность детей в интернете и защитить их от рисков, которые наступят завтра?

Этот вопрос нужно обсуждать на всех уровнях: от бытового, в рамках каждой семьи, до государственного, развивая пространство для совместной ответственности за безопасность детей. Например, ИТ-разработчикам необходимо сконцентрироваться на рисках, противодействие которым недостаточно эффективно. А бизнес и все коммерческие предприятия должны сделать безопасность детей приоритетом, учитывая её ещё на стадии разработки продукта. Отдельно нужно отметить роль институтов образования. На мой взгляд, именно они должны стать центрами экспертизы по этой теме.

Особенно важно развивать у детей навыки цифровой гигиены и безопасного использования интернета. Однако по-настоящему эффективно защитить детей от киберрисков и предотвратить их появление можно только объединив усилия всех заинтересованных сторон. Такая работа уже ведется в рамках Альянса по защите детей в цифровой среде, одним из учредителей которого стал «Ростелеком». Компании-основатели альянса прилагают максимум усилий для создания безопасной и благоприятной цифровой среды, делятся лучшими практиками и новейшими разработками во благо самых молодых членов российского общества. Уверен, вместе крупнейшие российские компании смогут создать по-настоящему благоприятную среду для развития, обучения и безопасного общения детей в виртуальном пространстве».

Михаил Осеевский,
президент ПАО «Ростелеком»

Содержание

Введение

Интернет становится неотъемлемой частью нашей жизни. Уровень проникновения интернета в России — 89 %, а это 129,8 из 145,9 миллионов человек, причем дети и несовершеннолетние составляют 21,8 % от населения страны. За 2021 год количество пользователей интернета увеличилось на 4,7 %.[1] Дети буквально «рождаются со смартфоном в руке» и активно пользуются интернетом, при этом они относятся к наиболее уязвимой категории пользователей: их когнитивные способности, мировоззрение и навыки критического мышления находятся в процессе формирования.

Количество преступлений в киберпространстве растет. С каждым днем появляются новые механики, представляющие угрозу для детей и подростков в интернете, а старые методы защиты перестают работать. Помимо семьи, школы и правоохранительных органов важными элементами защиты детей становятся ИТ-решения, встроенные в привычную цифровую среду: поисковые системы, социальные сети, коммуникационные сервисы, игры.

Разработка технологических методов защиты детей, направленных на обеспечение их безопасности в онлайн-среде, неразрывно связана с изучением киберрисков, представляющих угрозу для несовершеннолетних.

Исследование «Технологии защиты детей в интернете» проводилось с октября 2021 года по апрель 2022 года. В рамках исследования был проведен анализ киберрисков для детей и подростков, изучены технологические меры по противодействию киберрискам, определены риски, с которыми несовершеннолетние могут столкнуться в будущем, а также предложены рекомендации для стейкхолдеров.

23 риска

8 кластеров

10 рисков в будущем

1 Digital 2022 Global Overview Report», We Are Social, Hootsuite, 2022

>> В основе исследования использовался искусственный интеллект (машинное обучение). Представленная информация и выводы получены с применением интеллектуальной аналитической системы выявления новых рынков, перспективных технологий и методов их использования TeqViser. Кластерный анализ проводился на основе выборки, включающей более 21 тысячи научных работ.

>> На основе анализа более 500 источников литературы было выявлено 23 риска, угрожающих безопасности детей и подростков в интернете. Для определения степени опасности рисков и эффективности технологических решений по противодействию им была дана экспертная оценка от приглашенных к исследованию специалистов в области кибербезопасности, детской психологии и социологии.

>> В рамках изучения технологических мер по противодействию киберрискам для детей и подростков было проанализировано более 300 патентов, компаний и ИТ-решений в области кибербезопасности детей и подростков. По результатам анализа было сформировано 8 кластеров технологических решений.

>> На основании существующих рисков и ряда трендов, продиктованных технологическими, социальными и геополитическими изменениями, были определены 10 областей, в которых будут формироваться риски для несовершеннолетних в ближайшем будущем.

>> По результатам исследования были предложены рекомендации для стейкхолдеров, направленные на усиление безопасности детей и подростков в интернете.

Ключевые выводы

1 Самые опасные риски связаны с психологическим насилием над ребенком

Риски, представляющие собой результат агрессивного столкновения между людьми, имеют высокую степень опасности. При этом технологические решения достаточно развиты, чтобы противостоять примитивным личностным атакам и снижать их объем, но не способны предотвратить атаки со стороны большого количества злоумышленников или тех, кто хорошо осведомлен о принципах работы технологии.

2 Решения, связанные с фильтрацией контента и защитой детей от онлайн-мошенничества, проработаны лучше других

Наиболее эффективно работают методы защиты от рисков, связанные с фильтрацией и блокировкой контента порнографического и насильственного характера, а также с предотвращением случаев онлайн-мошенничества и распространения опасных товаров. Технологические решения, направленные на противодействие этим рискам, встроены в функционал сразу нескольких кластеров технологических мер борьбы (системы родительского контроля, интернет-фильтры), а также присутствуют непосредственно на платформах, предоставляющих цифровой контент.

3 Недооценены риски, связанные с информационным и маркетинговым давлением

Риски, связанные с информационным и маркетинговым давлением, вовлечением детей в рискованные денежные отношения, а также распространением дезинформации и контента, не предназначенного для детей и подростков, в значительной степени недооценены. Хотя стейкхолдеры информированы об их наличии, необходимо повышение цифровой грамотности в области их профилактики, а также консолидации усилий со стороны всех вовлеченных сторон.

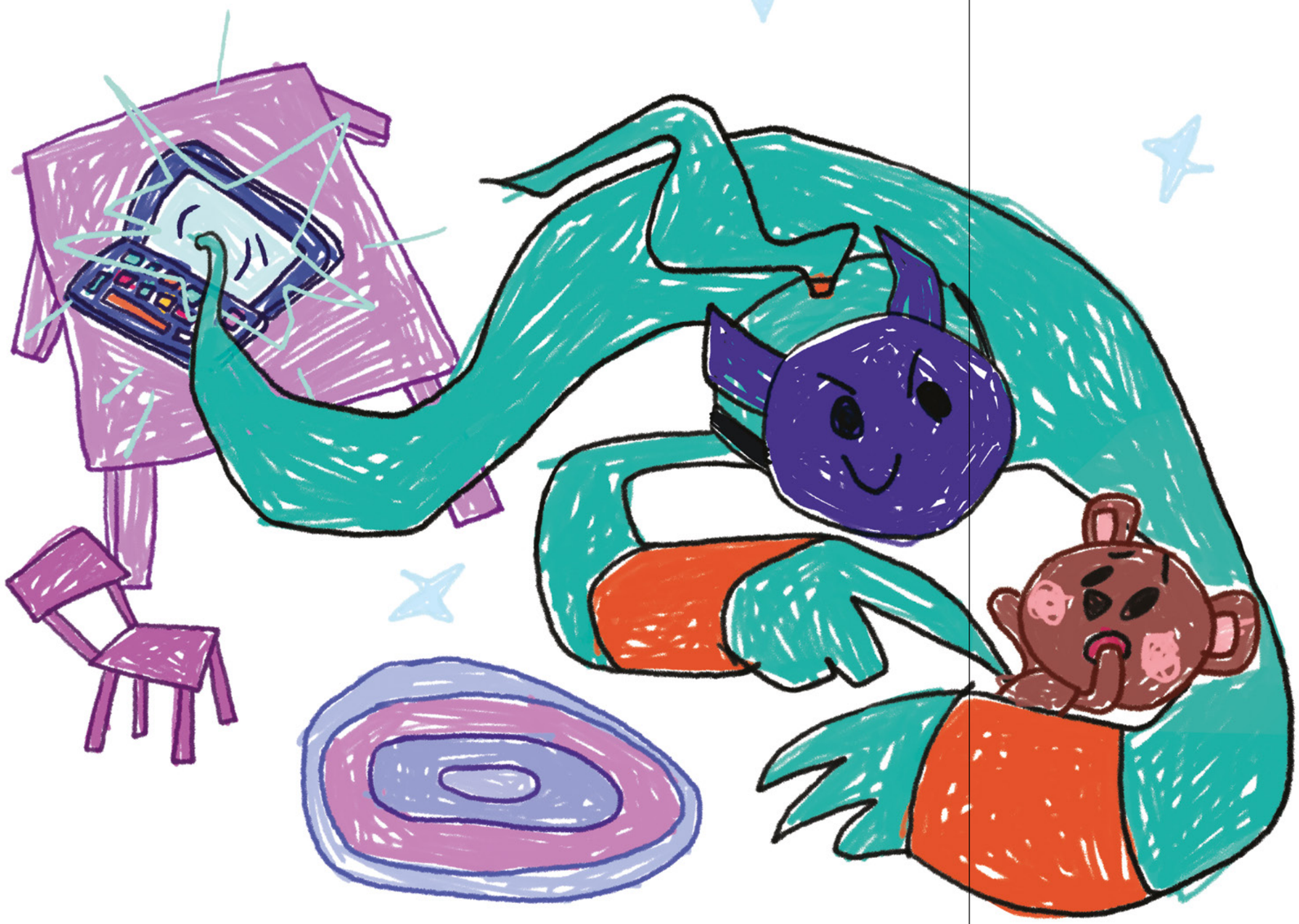
4 Риски будущего требуют особого внимания

В среднесрочной перспективе ожидается усиление рисков, связанных с развитием виртуальной реальности и метавселенных (рост влияния цифровых инфлюенсеров, новые возможности взаимодействия между взрослыми и детьми); искусственного интеллекта как инструмента преступной деятельности и технологии воспитания; ростом цифрового разрыва, информационных войн и цифровой изоляции; новыми угрозами приватности и персональным данным (цифровой след, биометрия).

5 Борьба с киберугрозами требует взаимодействия множества стейкхолдеров

Развитие технологий как порождающих киберриски, так и направленных на борьбу с ними, происходит крайне динамично. В процесс поиска решений в этой сфере должно быть вовлечено множество субъектов. При этом стейкхолдеры должны быть свободны в проявлении инициативы и экспериментировании. Процесс будет по-настоящему эффективным в том случае, если будет сформировано пространство совместной ответственности за результат.

Киберриски для детей и подростков



1

>>

Для того чтобы определить, с какими рисками дети и подростки могут столкнуться в интернете, использовался кластерный анализ на основе выборки, включающей более 21 тысячи научных работ.

>> КЛАСТЕРЫ РЕЛЕВАНТНЫХ НАУЧНЫХ РАБОТ

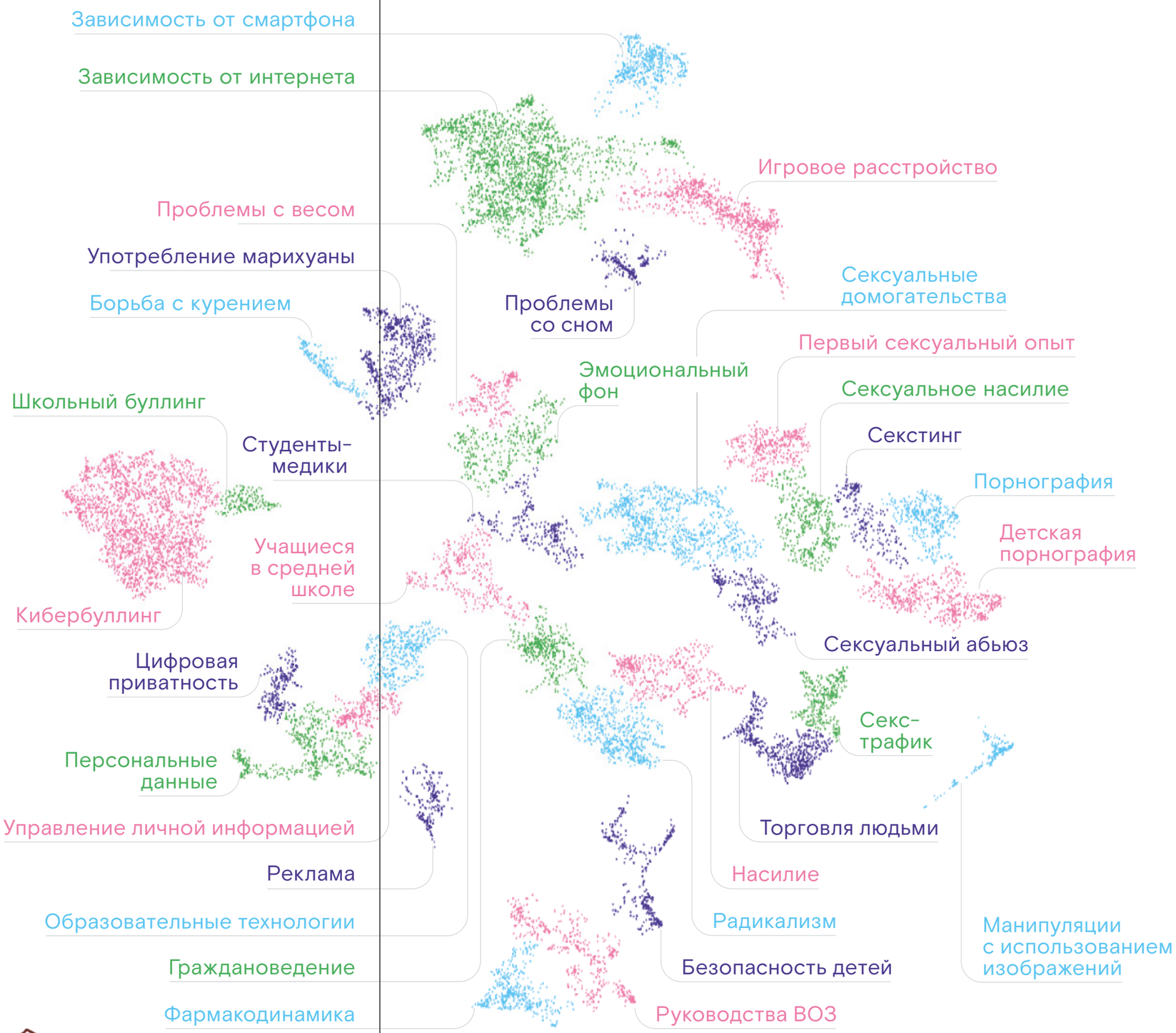
Кластеризация представляет собой разбиение выборки объектов на подмножества, называемые кластерами, так, чтобы каждый кластер состоял из схожих объектов. Каждая точка на карте представляет собой одну из научных статей, которые объединены в кластеры по принадлежности к определенной тематике.

Всего было выделено 33 кластера релевантных научных работ. К наиболее крупным кластерам, привлекающим внимание исследователей, можно отнести: кибербуллинг, интернет-зависимость и риски сексуального характера (домогательства, порнографический контент), трафикинг, а также риски, касающиеся безопасности персональных данных детей.

33

кластера
релевантных
научных работ

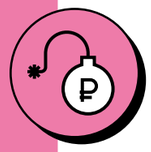
Затем мы проанализировали более 500 отечественных и зарубежных источников литературы, в результате чего выделили 23 ключевых киберриска для несовершеннолетних и сгруппировали их в 6 блоков.



>> КИБЕРРИСКИ ДЛЯ ДЕТЕЙ И ПОДРОСТКОВ

Криминализация, втягивание в криминальные практики

1. Вовлечение детей в криминальные сообщества
2. Продажа запрещенных товаров и услуг
3. Радикализация и экстремизм
4. Траффикинг



Маркетинговое давление, рискованные денежные отношения

5. Интернет как канал сбыта товаров, опасных для жизни и здоровья детей
6. Продвинутые методики маркетинга
7. Темные паттерны
8. Онлайн-мошенничество

Личностная атака, психологическое насилие

9. Кибербуллинг
10. Сталкинг
11. Груминг
12. Сексуальные домогательства

Цифровая эксплуатация, использование ребенка для создания цифрового контента

13. Доксинг
14. Создание и распространение материалов с детской порнографией
15. Кража, сбор и эксплуатация персональных данных
16. Шерентинг

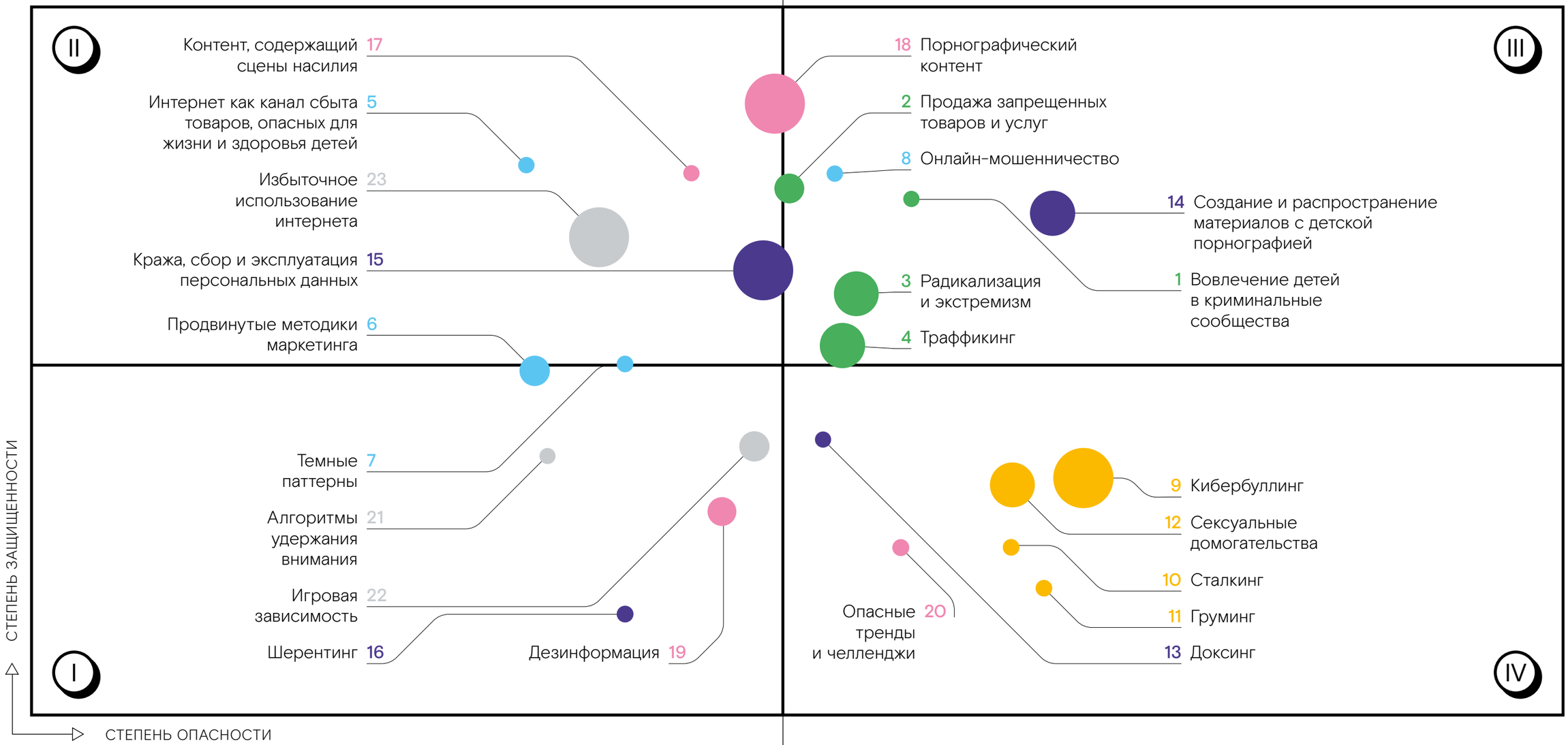
Информационное давление, информация, не предназначенная для детей и подростков

17. Контент, содержащий сцены насилия
18. Порнографический контент
19. Дезинформация
20. Опасные тренды и челленджи

Аддикция, формирование зависимости от интернет-среды

21. Алгоритмы удержания внимания
22. Игровая зависимость
23. Избыточное использование интернета

>> КАРТА РИСКОВ



- Криминализация, втягивание в криминальные практики
- Маркетинговое давление, рискованные денежные отношения
- Личностная атака, психологическое насилие
- Цифровая эксплуатация, использование ребенка для создания цифрового контента
- Информационное давление, информация, не предназначенная для детей и подростков
- Аддикция, формирование зависимости от интернет-среды

Количество упоминаний конкретного риска для детей и подростков в новостях и научных работах (определялось с помощью TeqViser).

В рамках исследования был проведен экспертный опрос, в ходе которого эксперты оценили степень опасности и степень эффективности технологических мер защиты (степень защищенности) каждого риска.
По результатам опроса мы расположили все киберриски по двум осям: «степень опасности» (ось X), «степень защищенности» (ось Y).

Таким образом, мы выделили 4 группы рисков:

I **НЕДООЦЕНЕННЫЕ** — риски с низкими степенями опасности и защищенности

II **КОНТРОЛИРУЕМЫЕ** — риски с низкой опасностью и высокой защищенностью

III **АКТУАЛЬНЫЕ** — риски с высокими степенями опасности и защищенности

IV **ТРЕБУЮЩИЕ ВНИМАНИЯ** — риски с высокой опасностью и низкой защищенностью

Криминализация, втягивание в криминальные практики

К этой группе относятся риски, которые подразумевают вовлечение детей в криминальные, запрещенные законодательством практики, например: вовлечение детей в криминальные сообщества, продажу запрещенных товаров и услуг, радикализацию и экстремизм, а также траффикинг.[2]

Последствия таких рисков могут крайне негативно сказаться на психоэмоциональном и физическом состоянии ребенка, а также представляют опасность для общества в целом.

2 Таффикинг — торговля людьми

1 >> ВОВЛЕЧЕНИЕ ДЕТЕЙ В КРИМИНАЛЬНЫЕ СООБЩЕСТВА

Детям, состоящим в группах и сообществах, пропагандирующих деструктивные действия, активно навязываются безнравственные ценности и установки. Например, обесценивание человеческой жизни, проявление агрессии и жестокости.

При этом подобные сообщества вовлекают несовершеннолетних в наркоманию, тематику социопатии, массовых и ритуальных убийств, сатанизма, анархии, нацизма, экстремизма.

Не единичны случаи вербовки людей в террористические организации через интернет, что приводит к распространению террористической идеологии на территориях отдельных стран, а также угрожает безопасности и жизнедеятельности общества в целом.

2 >> ПРОДАЖА ЗАПРЕЩЕННЫХ ТОВАРОВ И УСЛУГ

Интернет дает возможность приобретать товары и услуги, свободная реализация которых запрещена или ограничена законодательством. Наиболее популярный запрещенный товар, который несовершеннолетние покупают через интернет — наркотики.

Кроме того, в интернете подростки могут приобрести нелегальное оружие, заказать услуги по взлому компьютеров, телефонов, аккаунтов в соцсетях и приложениях. Обычно для этого используют даркнет,[3] обеспечивающий анонимность покупателя и продавца.

Детям и подросткам сложнее, чем взрослым, придерживаться правил поведения и моральных ценностей в интернете. Они могут приобретать запрещенные товары и услуги из любопытства или ради чувства причастности к определенной группе людей.

3 >> РАДИКАЛИЗАЦИЯ И ЭКСТРЕМИЗМ

Подростки в возрасте от 14 до 17 лет наиболее восприимчивы к радикальным националистическим, ксенофобским и экстремистским идеям. Часто в экстремистские и радикальные организации вербуют через социальные сети.

Кроме того, алгоритмы рекомендательных сервисов настроены на показ информации в зависимости от интересов пользователя. Если ребенок заинтересовался радикализацией определенной формы, вероятность того, что алгоритмы порекомендуют контраргументы, способные его переубедить, крайне мала. Система может направить пользователя к сообществам радикалов, каналам пропаганды и материалам, которые только углубят его наклонности и укрепят экстремистские взгляды.

3 Даркнет (DarkNet) — сегмент интернета, который скрыт из общего доступа

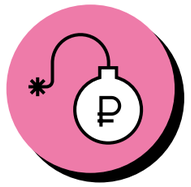
4 >> ТРАФФИКИНГ

Жертв траффикинга или торговли людьми, большинство из которых женщины и подростки, принуждают к проституции, насильно заставляют работать, убивают для продажи органов на трансплантацию, незаконно усыновляют (удочеряют).

Помимо этого, интернет открыл новые формы работы и коммерциализации. Например, видеотрансляции в реальном времени, в которых преступник получает деньги за бесчеловечные действия по отношению к ребенку.

Преступники могут находить потенциальных жертв в онлайн-чатах, для этого они занимаются развитием сообществ, профилированием жертв, и даже используют рекламу. Интернет также дает возможность находить покупателей — рекламировать жертв траффикинга, привлекать клиентов и сообщников. При этом реальные данные преступников и история их злодеяний скрыта за барьерами закрытых сообществ и в даркнете.

Маркетинговое давление, рискованные денежные отношения



К этой группе относятся риски, в основе которых лежат маркетинговые инструменты, паттерны поведения и тонкие психологические уловки, созданные для манипуляции детьми, например: сбыт товаров, опасных для жизни и здоровья детей, продвинутые методики маркетинга, темные паттерны и онлайн-мошенничество.

Маркетинговые, психологические и дизайнерские инструменты, использующиеся как законно, так и незаконно, чаще всего нацелены на извлечение финансовой выгоды, однако в некоторых случаях могут привести и к другим серьезным последствиям.

5 >> ИНТЕРНЕТ КАК КАНАЛ СБЫТА ТОВАРОВ, ОПАСНЫХ ДЛЯ ЖИЗНИ И ЗДОРОВЬЯ ДЕТЕЙ

Дети формируют собственный рынок сбыта и убеждают родителей приобретать определенные товары, например, продукты питания, игрушки, одежду и обувь, косметику, электронику и канцелярские товары. В то же время, они не способны проанализировать качество потенциальной покупки, а родители не всегда тщательно проверяют купленные товары.

Реклама и продажа детям некачественных, опасных товаров может привести к целому спектру негативных последствий — в первую очередь, они касаются здоровья ребенка.

В некоторых случаях детские товары содержат токсичные вещества в концентрации, в несколько раз превышающей допустимую. Они раздражают кожу и слизистую оболочку, отрицательно воздействуют на репродуктивную функцию человека, могут вызвать аллергию и даже рак.

6 >> ПРОДВИНУТЫЕ МЕТОДИКИ МАРКЕТИНГА

Передовые маркетинговые стратегии помогают компаниям выстраивать отношения с клиентами, в том числе с детьми.

Дети — желанная цель для маркетологов. Компании применяют сложные алгоритмы для нацеливания рекламы на детей в социальных сетях и играх, например, датамайнинг и профилирование. При этом персональные данные и профили детей доступны для покупки бизнесом.

Дети склонны покупать на карманные деньги то, что им рекламируется. При этом даже если дети не могут самостоятельно приобретать товары, они способны убеждать своих родителей на совершение таких покупок.

7 >> ТЕМНЫЕ ПАТТЕРНЫ

Темные паттерны — это тонкие психологические уловки и дизайнерские решения, которые намеренно подталкивают пользователей на выполнение определенных действий, поощряя постоянное совершение покупок.

Существует множество методов манипулятивного дизайна, которые подталкивают пользователей сделать то, чего в противном случае они бы не стали делать. Эти методы получили широкое распространение в последние годы, и в настоящее время компании широко применяют их на детскую аудиторию.

Воздействие темных паттернов усугубляется тем, что дети не могут защитить себя от них, так как не обладают необходимыми когнитивными и аналитическими способностями. Они уязвимы, склонны к импульсивному поведению, легко формируют отношения с персонажами, поддаются влиянию вознаграждений и статусов, при этом у них еще не сформировано зрелое понимание о ценности денег и недостаточно высокий уровень финансовой грамотности.

8 >> ОНЛАЙН-МОШЕННИЧЕСТВО

Интернет-сервисы или программное обеспечение с доступом в интернет может использоваться для обмана жертв. К видам онлайн-мошенничества можно отнести фишинг, лотереи, подарочные акции, спам с заманчивыми предложениями, поддельные кошельки платежных систем и всевозможные их комбинации.

В связи с тем, что дети и подростки наиболее подвержены внушению, а их психоэмоциональные особенности находятся на стадии созревания, они являются одной из наиболее уязвимых категорией жертв для онлайн-мошенников.

Последствия онлайн-мошенничества имеют как финансовые, так и социально-психологические последствия, включающие в себя ощущение разочарования и несправедливости, стресс.

Личностная атака, психологическое насилие

К этой группе относятся риски, конечная цель которых — нанести моральный, физический или иной ущерб конкретному ребенку, например: кибербуллинг, сталкинг, груминг и сексуальные домогательства.

В случае наступления этих рисков, жертвой становится конкретный ребенок, а злоумышленник проявляет целенаправленную агрессию в его сторону или предпринимает попытки использовать ребенка в корыстных и противоправных целях.

9 >> КИБЕРБУЛЛИНГ

Кибербуллинг подразумевает повторяющиеся эпизоды агрессивного поведения, направленные на то, чтобы напугать, унизить или разозлить человека. Такая форма поведения встречается в социальных сетях, мессенджерах, игровых платформах и других онлайн-площадках. Кибербуллинг может совершаться и детьми, и взрослыми.

Обидчики в киберпространстве более жестоки из-за анонимности — их сложнее выявить и привлечь к ответственности. Кроме того, они не видят жертву, а поэтому не видят последствий и результатов своих действий, что только усугубляет ситуацию.

Кибербуллинг негативно влияет на поведение, психоэмоциональное и физическое здоровье жертвы. Изменения в эмоциональном состоянии характеризуются резкой переменой настроения в сторону негативных эмоций — злости, раздражительности, уныния, боязливости, одиночества. Конкретный эмоциональный эффект и тяжесть последствий зависят от ребенка, но в крайних случаях кибербуллинг может стать даже причиной самоубийства.

10 >> СТАЛКИНГ

Сталкинг — паттерн поведения, проявляющийся в навязчивом преследовании, выслеживании и продолжительных домогательствах до жертвы. Отличается высокой длительностью, пристальным вниманием к действиям жертвы.

Сталкер может использовать широкий спектр тактик и подходов в своих домогательствах и слежке за жертвой. Например, обычные и электронные письма, звонки, сообщения и другие действия в соцсетях, установка программного обеспечения для мониторинга на устройства жертвы.

Сталкинг вызывает у жертвы спектр негативных эмоций, главными из которых являются страх и ощущение потери контроля над жизнью.

11 >> ГРУМИНГ

Груминг — это установление дружеского и эмоционального контакта с ребенком для его дальнейшей сексуальной или криминальной эксплуатации, мошенничества, шантажа, компрометирования или домогательств.

Онлайн-грумеры собирают информацию о детях и находят наиболее уязвимых жертв. Они знакомятся сразу с несколькими детьми, а затем выбирают свою жертву из тех, кто отреагировал на их сообщения, и анализируют соцсети ребенка, например, на предмет одиночества, нехватки внимания и заботы. После этого грумеры устанавливают психологический контакт с ребенком для дальнейшей реализации своих целей.

12 >> СЕКСУАЛЬНЫЕ ДОМОГАТЕЛЬСТВА

Сексуальные домогательства включают в себя запугивание, издевательство или принуждение сексуального характера, а также нежелательное или ненадлежащее обещание вознаграждения в обмен на сексуальные услуги, иные устные или физические преследования сексуального характера.

К особенностям сексуальных домогательств в интернете также относят нежелательное половое поведение, выражаемое в использовании цифрового контента в частных переписках или на публичных платформах. Например, обмен изображениями и видео сексуального характера, принуждение и угрозы, издевательства на сексуальной почве.

У детей, которые становятся жертвами сексуального домогательства в интернете, проявляются серьезные отклонения в физическом и психологическом здоровье. Для каждой жертвы, подвергшейся домогательству, эти последствия уникальны, а восстановление может длиться всю жизнь. Домогательство в интернете может переходить в офлайн и принимать самую критическую форму — изнасилование.

Цифровая эксплуатация, использование ребенка для создания цифрового контента

К этой группе относятся риски, которые напрямую связаны с эксплуатацией ребенка или информации о нем в интернете, например: доксинг, создание и распространение материалов с детской порнографией, кража, сбор и эксплуатация персональных данных, а также шерентинг.

Так, персональные данные ребенка могут быть раскрыты и/или использованы неправомерно, что повлечет за собой угрозы его физическому, психоэмоциональному или финансовому благополучию. При этом ребенка могут использовать для создания цифрового контента самыми разными способами — от фотографий в блоге родителей, до незаконной эксплуатации детей в производстве материалов сексуального характера.

13 >> ДОКСИНГ

Доксинг — публичное раскрытие в сети персональной информации о человеке или группе людей. К такой информации может относиться, например, настоящее имя, адрес проживания, места работы, данные родственников, номера телефонов, финансовая, медицинская и другая идентифицирующая информация.

Иногда под доксингом подразумевается не только публикация данных, но и процесс подготовки — сбор информации о жертве и близких жертвы посредством использования соцсетей, государственных отчетов, поисковиков и других источников информации.

Личная информация ребенка публикуется и распространяется без его согласия. Доксинг обычно производится намеренно, с целью отомстить, запугать, шантажировать или иным образом навредить жертве.

14 >> СОЗДАНИЕ И РАСПРОСТРАНЕНИЕ МАТЕРИАЛОВ С ДЕТСКОЙ ПОРНОГРАФИЕЙ

С развитием технологий порнографические материалы о детях в больших количествах создаются и передаются преступниками по всему миру.

Невозможно определить, сколько людей потребляет детскую порнографию, точно так же, как невозможно точно определить, сколько детей становятся жертвами детской порнографии.

Последствия для детей, ставших жертвами, крайне серьезны. Такие преступления напрямую связаны с насилием над детьми. А тот факт, что жестокое обращение было записано и распространено, усугубляет ситуацию: травма усиливается знанием того, что записанное и изображенное насилие распространяется и доставляет удовольствие другим.

15 >> КРАЖА, СБОР И ЭКСПЛУАТАЦИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

Эксплуатация персональных данных подразумевает получение доступа к личным данным детей и сбор этой информации незаконным способом, а также без согласия самих детей и их родителей, включая дальнейшее неправомерное использование. Также к данному риску относятся данные, полученные законным путем, но использующиеся в корыстных целях.

Чаще всего дети сами указывают личную информацию в интернете и свободно делятся ей с другими людьми. При этом они считают конфиденциальной информацией только контактные данные и не испытывают беспокойства за фото- и видеоконтент, который публикуют.

Доступ к личным данным открывает возможности для других правонарушений и рисков, связанных с опасностью для психического и физического здоровья жертвы.

16 >> ШЕРЕНТИНГ

Шерентинг — это регулярное использование родителями социальных сетей для обмена новостями, изображениями и другой информацией о детях. Слово образовано от английских слов «share» — делиться, и «parenting» — воспитывать, растить ребенка.

Дети зачастую испытывают неловкость, когда родители публикуют их фотографии. Они также испытывают беспокойство по поводу того, что они никак не могут повлиять на публикацию фотографий их родителями.

Шерентинг может привести к искажению представлений о реальной жизни. Родители высказывают свою точку зрения, зачастую не спрашивая, что об этом думает сам ребенок. Публикуя посты о своих детях, родители сами создают цифровой портрет ребенка в интернете, тем самым вмешиваясь в его цифровую идентичность. Помимо того, что родители публикуют фотографии своих детей и истории, связанные с их воспитанием, они также раскрывают конфиденциальную информацию о своих детях, которая может включать полное имя детей, дату рождения, вес, рост, геолокацию и другие данные.

Информационное давление, информация, не предназначенная для детей и подростков

К этой группе относятся риски, в основе которых лежит информация, способная травмировать, дезинформировать, подтолкнуть ребенка к неверным выводам или опасным действиям, например: контент, содержащий сцены насилия, порнографический контент, дезинформация, а также опасные тренды и челленджи.

Последствия таких рисков могут крайне негативно сказаться на психоэмоциональном и физическом состоянии ребенка, а также представляют опасность для общества в целом.

17 >> КОНТЕНТ, СОДЕРЖАЩИЙ СЦЕНЫ НАСИЛИЯ

К такого рода контенту относится любая доступная для восприятия форма представления информации, воспроизводящая ситуации или действия насильственного характера, которые причиняют или могут причинить вред одному или нескольким лицам.

Дети учатся, наблюдая и пробуя поведенческие сценарии, поэтому они особенно восприимчивы к негативным последствиям, которые вызывает потребление контента с насилием.

Краткосрочные эффекты связаны с процессами возбуждения и непосредственной имитацией определенного поведения. Долгосрочные эффекты обусловлены более продолжительным изучением такого контента, из-за чего негативные эмоции детей по отношению к насилию постепенно уменьшаются, и формируются новые установки.

18 >> ПОРНОГРАФИЧЕСКИЙ КОНТЕНТ

Интернет считается ключевым каналом распространения порнографического контента. При этом дети и подростки могут сталкиваться с порнографией умышленно и неумышленно.

Умышленный поиск и потребление возможны из-за того, что механизмы верификации возраста в соцсетях и на сайтах с такого рода контентом несовершенны. Среди причин непреднамеренного

столкновения с порнографией выделяют изучение смежных с сексом тематик, например, взаимоотношений между мужчиной и женщиной.

При встрече с порнографическими материалами часть детей испытывает отвращение, замешательство и тревогу, но с каждым разом эти ощущения становятся слабее. Это влияет на психическое здоровье и благополучие, в том числе столкновения с порнографией являются предиктором повышенной сексуальной агрессии и несерьезного отношения к сексуальным контактам.

19 >> ДЕЗИНФОРМАЦИЯ

Дезинформация — это попытка создать ложное впечатление и подтолкнуть объект воздействия к желаемым действиям или бездействию. Это процесс манипулирования информацией, например, введение кого-либо в заблуждение путем предоставления неполной или вырванной из контекста информации, искажения части информации, распространение слухов, лжи и громких, но не подкрепленных фактами утверждений.

Интернет считается главным каналом и инструментом распространения дезинформации. При этом дети могут быть особенно уязвимы в вопросах восприятия информации, поскольку их мышление и когнитивные способности все еще развиваются.

Дети не могут оценить достоверность информации, с которой они сталкиваются в интернете. Это может привести к формированию у них ложной картины мира, совершению некорректных действий по отношению к себе и окружающим.

20 >> ОПАСНЫЕ ТРЕНДЫ И ЧЕЛЛЕНДЖИ

Тренды и челленджи вовлекают детей и подростков в массовые активности, которые могут угрожать психическому и физическому здоровью участников или окружающих, через социальные сети и обмен сообщениям в мессенджерах. Вовлечение происходит путем приглашения аудитории в игру или соревнование с выполнением заданий, отчетами в фото- и видеоформате или онлайн-трансляции.

В большинстве случаев участие в выполнении задач или игры приводит к опасным последствиям из-за непонимания реального риска и несформировавшегося критического мышления. Если подростки уже имеют какие-либо психологические проблемы, в том числе суицидальные наклонности, они находят опасные тренды, усугубляющее состояние, что в совокупности может привести к трагедии.

Среди последствий опасных трендов могут быть отравления, физические и психологические травмы, нанесенные себе и другим, и даже непреднамеренный летальный исход или суицид. Кроме того, опасные тренды могут способствовать сексуализации детей или вовлекать их в криминальные сообщества.

Аддикция, формирование зависимости от интернет-среды

К этой группе относятся риски, при наступлении которых у ребенка формируется зависимость от интернета в целом или конкретных его элементов, например: алгоритмы удержания внимания, игровая зависимость и избыточное использование интернета.

Последствия таких рисков заключаются в ухудшении общего самочувствия ребенка, его социальных связей, успеваемости. Нередко подобная зависимость приводит к отклонениям в поведении, отсутствию интереса к привычной жизни и депрессии.

21 >> АЛГОРИТМЫ УДЕРЖАНИЯ ВНИМАНИЯ

Алгоритмы анализируют реакции пользователя, считывают моментальный отклик на информацию, а затем подбирают похожий контент. Таким образом, они ограничивают поток информации до интересных пользователю публикаций, формируют рекомендации, показывают таргетированную рекламу.

Основная цель алгоритмов — удерживать внимание ребенка как можно дольше. Для этого используется множество маркетинговых инструментов, например, игровые петли, создающие эффект незавершенности действия и вызывающие синдром упущенных возможностей (FOMO, от англ. fear of missing out).

Показывая только то, что интересно пользователю, алгоритмы изначально проектируются на поляризацию мнений на любые темы, которые влияют

на становление мировоззрения детей и подростков. Система подбирает людей по интересам и убеждениям, объединяя их в группы. Этот эффект получил название «эхо-камеры»: пользователь окружен только той информацией и теми людьми, которые подтверждают одну точку зрения, подкрепляя его правоту. При этом между такими группами усиливается разница во взглядах и установках, что провоцирует агрессию и конфликты.

20 >> ИГРОВАЯ ЗАВИСИМОСТЬ

Игровая зависимость характеризуется постоянной, повторяющейся потерей контроля над игровым процессом, повышением приоритета игр над другими интересами и повседневной деятельностью ребенка, а также продолжением или эскалацией этой модели поведения, несмотря на возникновение негативных последствий.

Среди причин игровой зависимости выделяют повышение социального статуса. Так, статус персонажа и достижения в игре напрямую зависят от затраченного времени. При этом во многих играх есть платные внутриигровые предметы, которые дают пользователю преимущество, что оказывает сильное давление на неокрепшую психику детей и подростков и подталкивают их к покупкам.

Зависимость от игр вызывает различные проблемы с социальным, психологическим и даже физическим состоянием. Она приводит к нарушению классического социального взаимодействия ребенка с семьей и друзьями, меняет образ жизни, мешает академической успеваемости.

23 >> ИЗБЫТОЧНОЕ ИСПОЛЬЗОВАНИЕ ИНТЕРНЕТА

Избыточное использование интернета приводит к нарушению психологического, социального, личностного, академического или профессионального благосостояния человека. В частных случаях это перетекает в зависимость от интернета — у человека появляются неоправданная тревога и желание подключиться к сети как можно скорее.

К основным симптомам интернет-зависимости относится не только увеличение количества времени, проведенного в интернете, но и перепады настроения, чувство одиночества, беспокойство и раздражительность. Помимо этого, интернет-зависимые склонны отказываться от ответственности и отрицать проблемы. Такие подростки чаще всего не могут контролировать время, проведенное онлайн, а также не в состоянии сократить его самостоятельно.

У зависимых от интернета и социальных сетей подростков также наблюдается дисморфофобия — это психическое расстройство, при котором человек чрезмерно обеспокоен незначительным дефектом или особенностью своего тела. Фильтры, инструменты для ретуши и обработки фотографий формируют у детей и подростков неверные представления о внешности, что приводит к комплексам в реальной жизни.

Технологические решения по защите детей в интернете

2

>>

Для того чтобы определить спектр существующих технологических решений, направленных на обеспечение безопасности детей в интернете, мы проанализировали более 300 патентов, компаний и ИТ-решений в этой области. По результатам анализа было сформировано 8 кластеров технологических решений.

>> КЛАСТЕРЫ

Предиктивная аналитика

Предиктивная аналитика может быть использована для защиты детей в интернете путем определения лиц, находящихся под риском совершения преступления или становления жертвой преступления. Она позволяет прогнозировать и выявлять на ранней стадии риски различного характера, изучать и классифицировать источники риска и ранжировать их в соответствии с возрастными группами детей.

Предиктивные системы используют большие данные, статистические методы, а также искусственный интеллект и машинное обучение. Предиктивная аналитика подразумевает изучение онлайн-среды, в том числе алгоритмов, устройств и пользовательских привычек детей, а также профилирование и анализ графа связей. Однако это поднимает ряд этических вопросов об использовании персональных данных детей.

В ходе анализа информации выявляются предикторы — определенные признаки в паттерне поведения, являющиеся сигналом возможного риска. Ограничением в данном случае является сложность сбора релевантных данных, а также длительное обучение алгоритмов для построения прогнозных систем и возможные ошибки в результатах.

 # PrevBOT

Чат-бот, базирующийся на алгоритмах. Он помогает полиции в выявлении злоумышленников в чатах, мессенджерах и социальных сетях. Бот считывает чужие переписки и записывает их, а также может имитировать общение ребенка, что позволяет обнаружить злоумышленников. Лингвистическая модель робота позволяет определять пол, возраст и авторский почерк человека и соотносить его с базой киберпрофилированных аккаунтов других потенциальных преступников. Кроме того, так как робот умеет распознавать преступников и определять, какие цифровые пространства они оккупируют, его можно использовать как инструмент для определения опасных для детей сообществ.

Детские социальные сети

Детские социальные сети являются аналогом обычных социальных сетей, они способны обеспечить дополнительную безопасность и защиту от угроз, с которыми ребенок может столкнуться в интернете.

Социальные сети для детей защищены различными системами модерации и фильтрации, что позволяет блокировать публикацию грубого, жестокого, нежелательного для просмотра контента. Однако системы автоматической фильтрации контента даже в детских соцсетях несовершенны, а модераторы не всегда успевают отслеживать подобные инциденты.

Детские социальные сети также направлены на ограничение контактов детей со злоумышленниками и взрослыми людьми. Помимо этого, некоторые детские социальные сети предусматривают общение ребенка только с теми пользователями, которые были предварительно одобрены родителями или опекунами. При этом остается довольно высокая вероятность регистрации в детской социальной сети взрослого злоумышленника под видом ребенка.

GromSocial

Детская социальная сеть, которая учит детей укреплять уверенность и не принимать близко к сердцу злые комментарии. В GromSocial для регистрации нужно участие родителей, что позволяет свести к минимуму присутствие в ней взрослых злоумышленников. Как только социальная сеть активируется, к ребенку в друзья попадают 17 мультипликационных персонажей, за которыми стоят модераторы, готовые помочь по любым вопросам.

Практики разработки

Практики разработки включают в себя создание и улучшение функционала, касающегося детской безопасности в приложениях и на интернет-площадках.

Пользовательский интерфейс должен предоставлять возможность блокировки некоторых функций во избежание запуска нежелательных действий и защиты детей от просмотра неприемлемой информации. В качестве примера можно привести решения, которые обеспечивают соблюдение возрастных ограничений, оповещают о потенциально травмирующем содержании публикации или небезопасности определенных сайтов.

Зачастую существующие решения не блокируют, а лишь ограничиваются оповещением пользователей о возрастных ограничениях и содержании контента, в том числе о его потенциальной опасности. При этом ответственность за последующие действия на платформе, сайте или в приложении несет сам пользователь.

Deutsche Bank API Program (DBAPI)

Решение, которое помогает онлайн-продавцам взрослой продукции не допустить на свои сайты несовершеннолетних. Сертификат возраста DBAPI предлагает проверку, в основе которой лежат данные клиентов Deutsche Bank. Проверенная информация о возрасте пользователя в режиме реального времени поступает на сайт, что позволяет повысить достоверность данных о возрасте посетителей.

Инструменты родительского контроля и мониторинга

Инструменты родительского контроля предоставляют родителям повышенную степень контроля над действиями детей в онлайн- и офлайн-среде благодаря установке специального программного обеспечения на смартфоны, компьютеры и другие устройства ребенка.

В базовый функционал инструментов родительского контроля входит блокирование доступа к интернету, приложениям и играм, ограничение экранного времени, защита от ненадлежащего контента путем его фильтрации, отслеживание онлайн-активности, контактов и местоположения ребенка. Эти функции заключаются в проактивной регуляции и мониторинге действий ребенка в интернете, поэтому такие программы позволяют выявлять и заблаговременно минимизировать киберриски для детей. Несмотря на широкий спектр функций подобных программ, полная изоляция ребенка от киберрисков не будет способствовать выработке необходимых компетенций в области кибербезопасности, которые понадобятся ему в будущем.

Научные исследования также показывают, что инструменты родительского контроля, которые позволяют осуществлять постоянное наблюдение за ребенком, разрушают доверие к родителям, а в отдельных случаях даже могут повлечь психологические травмы и депрессию. В случае когда ребенок или подросток испытывает отторжение и непринятие инструментов родительского контроля, он может найти способы обхода установленных правил.

 # Kaspersky Safe Kids

Решение родительского контроля. Совместимо с Windows, macOS, Android и iOS. Функционал: блокировка нежелательного контента, ограничение доступа к устройствам в соответствии с расписанием, ограничение доступа к приложениям, составление списка приложений, доступ к которым осуществляется с разрешения родителей, отслеживание местоположения по GPS, безопасный поиск и история активности на YouTube, контроль уровня заряда батареи.

Интернет-фильтры

Одним из способов защиты детей в интернете является использование интернет-фильтров, которые блокируют доступ к нежелательным сайтам и скачивание файлов определенной тематики, ограничивают запуск приложений и игр.

Также существуют специальные программы, которые обеспечивают фильтрацию интернет-ресурсов по встречающимся ключевым словам без необходимости внесения родителями вручную в черный список отдельных сайтов с неприемлемым контентом для детей.

Такие фильтры не привязаны ко времени реагирования команды модераторов или нейросети, они защищают ребенка постоянно.

 # Lidrekon

Расширение для браузера, позволяющее фильтровать контент. Проверка контента происходит на основе российской библиотеки фильтров, которая постоянно обновляется. Фильтрует контент по темам: членовредительство, суицид, ПАВ, наркотики, табак, алкоголь, азартные игры, проституция, бродяжничество, оправдание насилия к людям и животным, отрицание семейных ценностей, нетрадиционные ориентации, неуважение к детям и родителям, криминал, оружие, нецензурная брань, порнография, экстремизм.

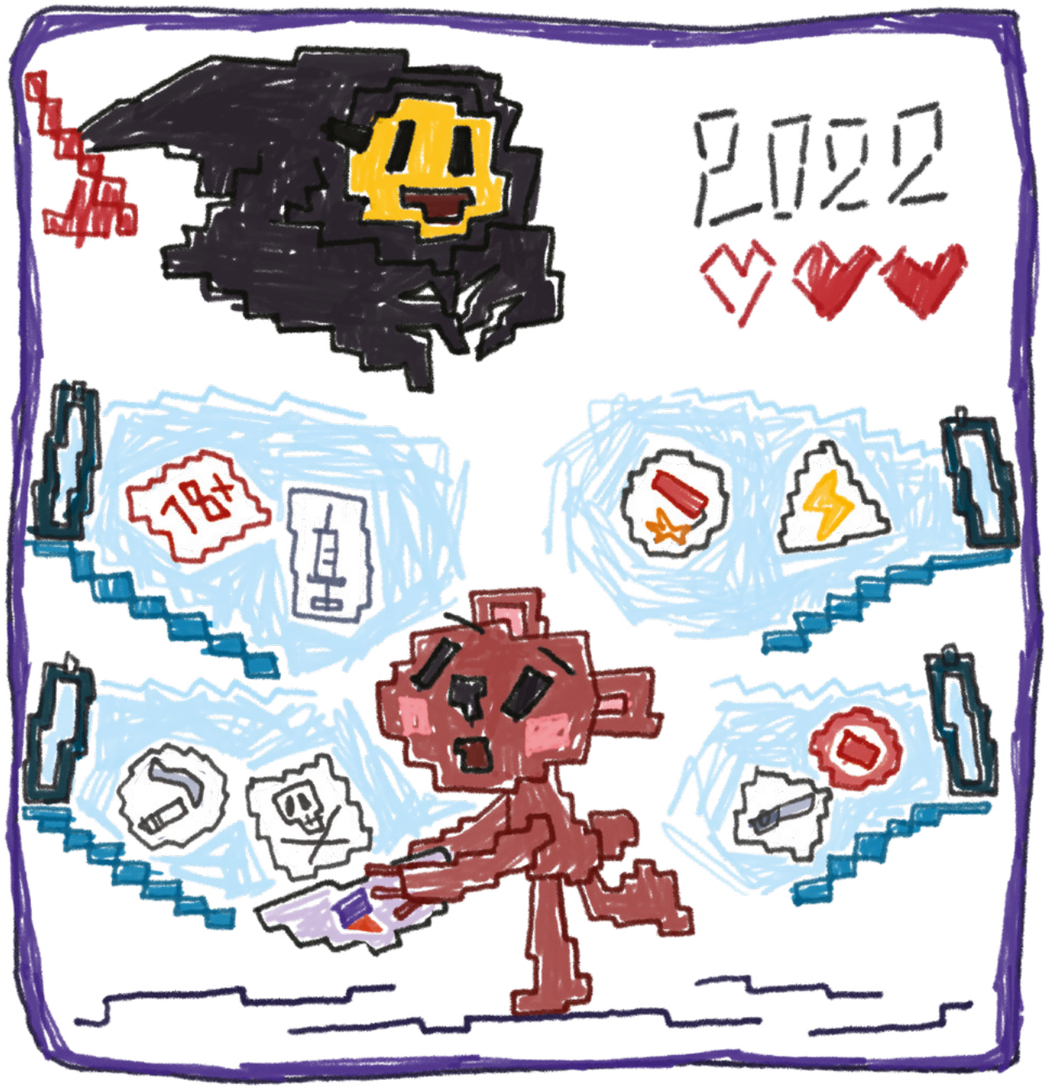
Автоматизированная модерация

Модерация контента подразумевает удаление информации, ее фильтрацию или блокировку, рекомендацию контента через новостные ленты, тематические списки и персонали-

зированные предложения, а также мониторинг контента.

Автоматизированная модерация контента может использоваться на соответствующих этапах превентивного обнаружения потенциально проблемного контента, а также для автоматизированной оценки и исполнения решения об удалении, маркировке или демаркировке, демонетизации или приоритизации контента. Автоматизация модерации позволяет значительно ускорить процесс, а также имеет более широкую область действия, например, возможность проверять контент в закрытых сообществах. Однако для обхода систем автомодерации широко используются варианты изменения данных, включающие в себя, например, введение дополнительных пробелов или полное их отсутствие, использование транслитерации и прочие способы.

При этом преимущество ручной модерации заключается в относительной точности, верифицируемости результатов удаления материалов, а также возможности улучшения критериев для блокировки. Механизмы автоматической фильтрации более действенны, однако они с большей вероятностью могут допускать ошибки при блокировке или удалении контента.



Meta[5]

Использует автомодерацию, чтобы выявлять спам, фейковые страницы, порнографию, экстремистские материалы, ролики со сценами жестокости. Однако на сегодняшний день алгоритмы не способны точно распознавать призывы к осуществлению экстремистской деятельности — этим занимаются модераторы. А в Instagram[5] внедрена программа DeepText на базе ИИ для фильтрации травли и издевательств. Изначально она искала только спам, потом научилась обнаруживать оскорбительные комментарии, а затем инструмент начали обучать анализу не только комментариев, но и постов.

Сервисы оказания помощи

Сервисы оказания помощи включают в себя спектр организаций и сервисов, которые позволяют ребенку, родителю или иным заинтересованным лицам запросить помощь психологов, волонтеров, правозащитников и других специалистов.

Они могут служить для оказания психологической помощи, коммуникаций между детьми и государством, НКО, волонтерами. Такие организации активно используют технологии и внедряются в инфраструктуру, которая касается поддержки детей. Одной из задач платформ реагирования также является просвещение общественности

5 Признаны экстремистскими организациями, деятельность которых запрещена на территории Российской Федерации

по вопросам помощи детям. При этом главными ограничениями таких служб являются компетентность специалистов и качество оказываемой помощи. Часто в подобных организациях работают волонтеры, которые не всегда могут правильно оказать помощь ребенку, столкнувшемуся с трудностями и рисками.

Многие платформы реагирования подразумевают несколько каналов для коммуникации с детьми, например, телефон доверия, сайты, мессенджеры или чат-боты. В зависимости от размеров и технических возможностей организации, количество и пропускная способность таких каналов варьируются.

Трудно подросткам

Чат-бот, позволяющий детям, пострадавшим от травли, обратиться за помощью. Бот способен перенаправлять запросы о помощи к организациям и индивидуальным специалистам. Он определяет проблему ребенка и потом направляет справочные материалы, контакты специалистов и профильных служб.

Инфраструктура

Под инфраструктурой подразумевается совокупность взаимосвязанных объектов, структур, решений в области безопасности, интегрированных в единую систему.

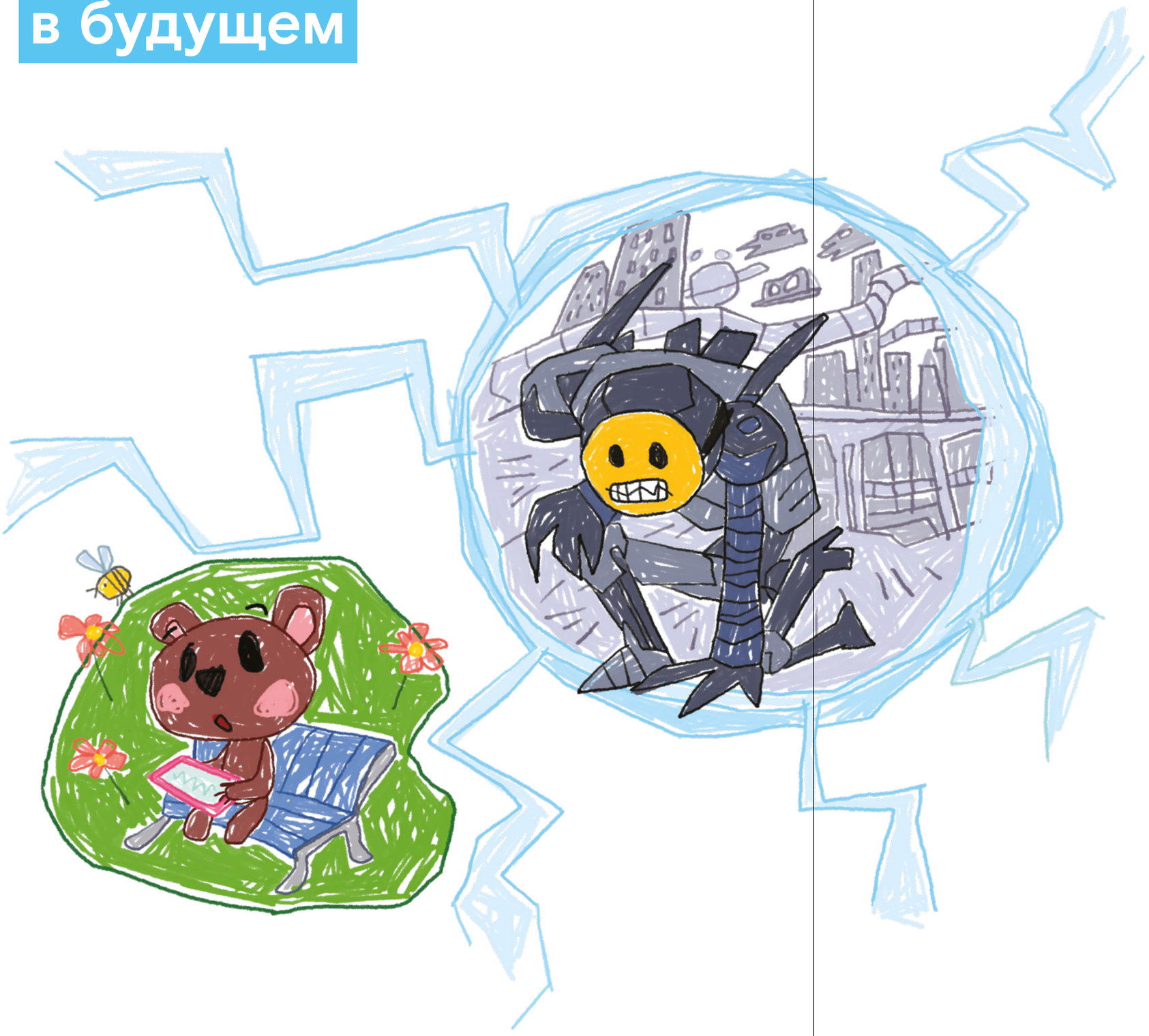
Основной принцип обеспечения безопасности — это непрерывность защиты в пространстве и времени.

Через системную интеграцию инфраструктура объединяет ресурсы и пространства. Под ресурсами понимаются различные технические и аппаратные средства, программное обеспечение и базы данных, каналы и средства связи. Пространства, в свою очередь, включают в себя различные физические объекты, начиная от места проживания ребенка, заканчивая общественными местами, транспортом, учебными заведениями и городом в целом.

AviaTor

Инфраструктурный проект INHOPE (международной ассоциации горячих линий интернета). INHOPE объединяет 50 горячих линий в 46 странах для борьбы с материалами, содержащими сексуальное насилие над детьми. Организация ежегодно обрабатывает тысячи запросов. AviaTor — это система, в рамках которой модераторы обрабатывают изображения, расставляя маркеры и хеши, фиксируя их в базе. Это позволяет автоматически выявлять аналогичные преступные материалы в интернете. INHOPE передает данные правоохранительным органам, что содействует поиску и поимке преступников, распространяющих такие материалы.

Риски в будущем



3

Цифровой мир стремительно меняется, поэтому на горизонте ближайших 5-10 лет можно спрогнозировать появление новых киберрисков для детей и подростков, связанных с развитием технологий, геополитическими изменениями и новыми трендами. Мы выделили 10 областей, в которых будут формироваться риски для несовершеннолетних в ближайшем будущем.

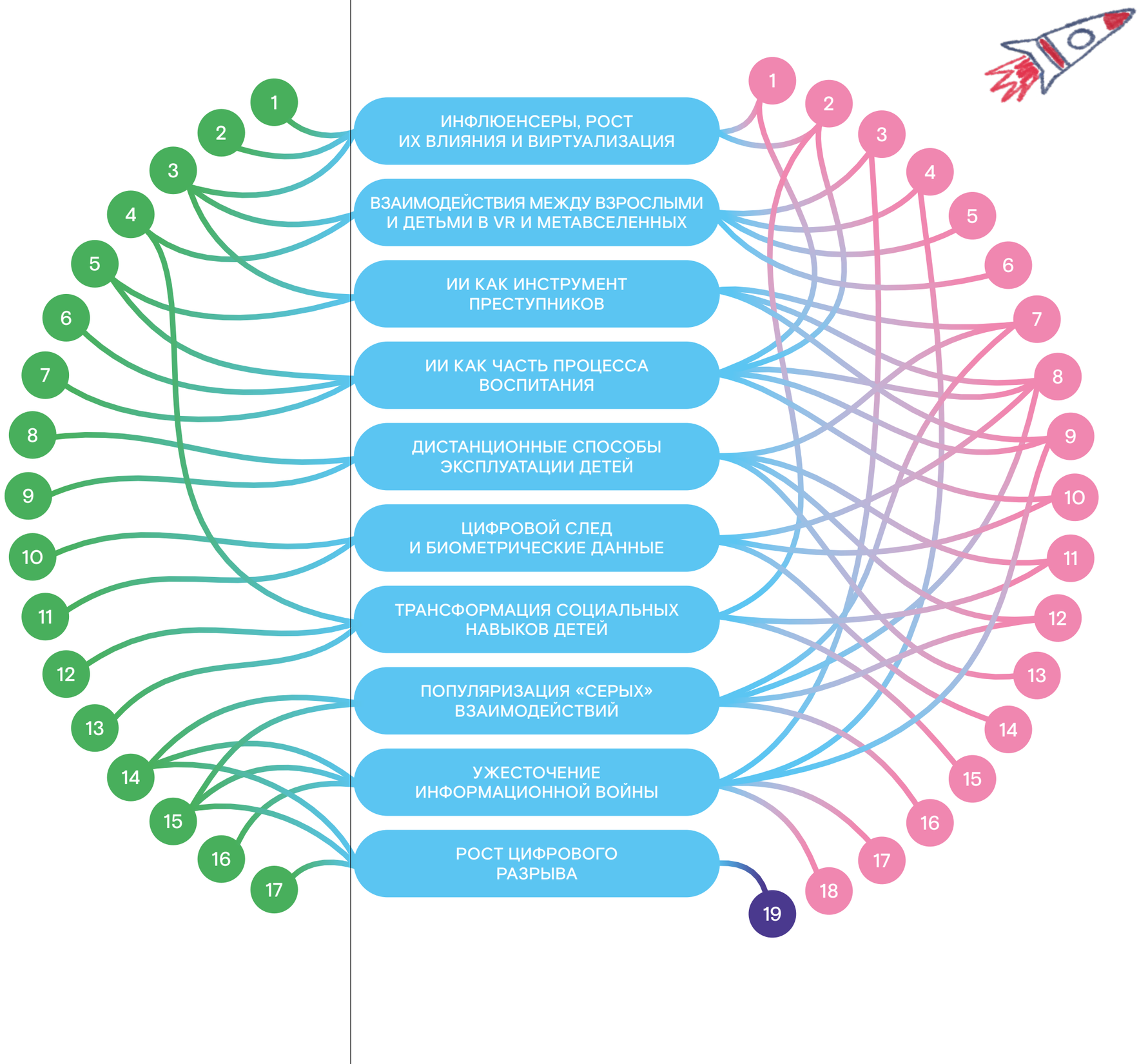
>> РИСКИ В БУДУЩЕМ

Тренды и технологии

1 Инфлюенсеры
2 Нейросети
3 VR
4 Метавселенные
5 Искусственный интеллект
6 Умные системы и гаджеты
7 Усиление влияния корпораций
8 Модели заработка в играх
9 Монетизация пользовательского контента
10 Биометрия
11 Большие данные
12 COVID-19 / социальная изоляция
13 Цифровизация общества
14 Геополитические изменения
15 Блокировка и некорректное регулирование интернет-ресурсов
16 Постправда
17 Социально-экономические изменения

Существующие риски

1 Опасные тренды и челленджи
2 Алгоритмы удержания внимания
3 Кибербуллинг
4 Сталкинг
5 Груминг
6 Сексуальные домогательства
7 Онлайн-мошенничество
8 Кража, сбор и эксплуатация персональных данных
9 Дезинформация
10 Продвинутые методики маркетинга
11 Игровая зависимость
12 Продажа запрещенных товаров и услуг
13 Темные паттерны
14 Шерентинг
15 Избыточное использование интернета
16 Вовлечение детей в криминальные сообщества
17 Доксинг
18 Радикализация и экстремизм
19 Включает все 23 риска



1 >> ИНФЛЮЕНСЕРЫ, РОСТ ИХ ВЛИЯНИЯ И ВИРТУАЛИЗАЦИЯ

Инфлюенсеры влияют на мнение и выбор детей и подростков, транслируют свои ценности и пользуются доверием со стороны аудитории, но не всегда осознают ответственность за это. При этом появляются полувиртуальные и виртуальные инфлюенсеры, за аватарами которых стоят неизвестные люди или организации, способные транслировать свои ценности и манипулировать доверием аудитории в различных целях.

2 >> ВЗАИМОДЕЙСТВИЯ МЕЖДУ ВЗРОСЛЫМИ И ДЕТЬМИ В ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ И МЕТАВСЕЛЕННЫХ

В современных VR-приложениях степень контроля за взаимодействием детей и взрослых низка — взрослые могут использовать аватары детей, а дети могут использовать аватары взрослых. С проникновением в нашу жизнь виртуальной реальности и метавселенных все больше людей разных возрастов будут выходить на одни и те же площадки. В VR уже отмечались прецеденты кибербуллинга, сексуальных домогательств и других действий, которые способны распространить сопутствующие риски на детей и подростков.

3 >> ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ИНСТРУМЕНТ ПРЕСТУПНИКОВ

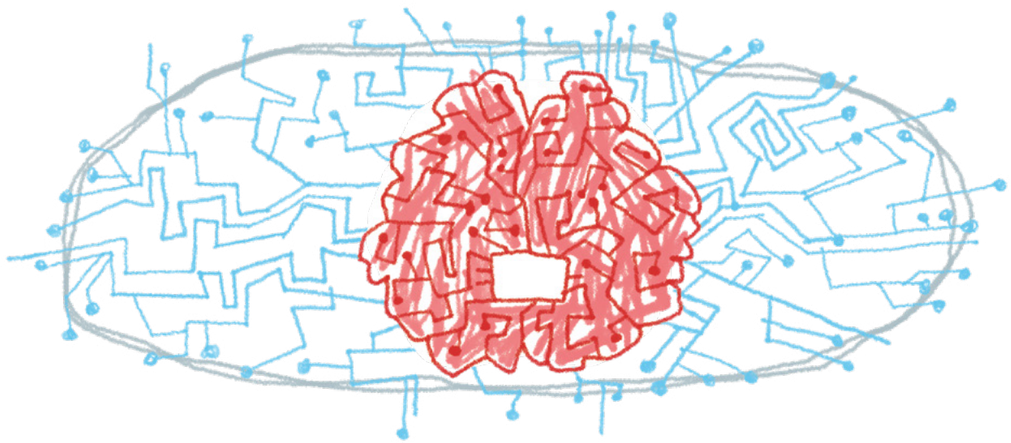
Коммодизация искусственного интеллекта, упрощение создания нейросетей и выход подобных технологий на потребительский рынок позволят злоумышленникам использовать их в качестве инструмента. Уже сейчас есть примеры систем, способных копировать лицо, голос и мимику — это может использоваться мошенниками для обхода систем, базирующихся на биометрической верификации. Подобные технологии позволяют агрессивно настроенному ребенку создать фото или видео, в которых сверстник находится в компрометирующей ситуации.

4 >> ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ЧАСТЬ ПРОЦЕССА ВОСПИТАНИЯ

Домашние голосовые ассистенты открывают новый вектор для вторжения корпораций в семью. Существует вероятность, что дети, пользующиеся ИИ-ассистентами как игрушками, станут жертвами создателей таких устройств. Создатели могут транслировать через них идеи, манипулировать алгоритмами подбора контента, собирать данные. Также возникает вопрос об осознании родителями беспрецедентной роли, которую корпорации начинают играть в воспитании их детей.

5 >> ДИСТАНЦИОННЫЕ СПОСОБЫ ЭКСПЛУАТАЦИИ ДЕТЕЙ

Одна из механик Web 2.0 — создание контента пользователями. Несовершеннолетние уже сейчас абсолютно бесплатно производят контент на платформах коммерческих компаний. Например, сотни часов групповой работы уходят на проекты в видеоигре Roblox, прибыль за которые получает компания, а не фактические создатели контента. Тема эксплуатации детского труда в интернете мало изучена, и взрослые редко понимают, по каким правилам функционирует сложная экосистема виртуального труда детей.

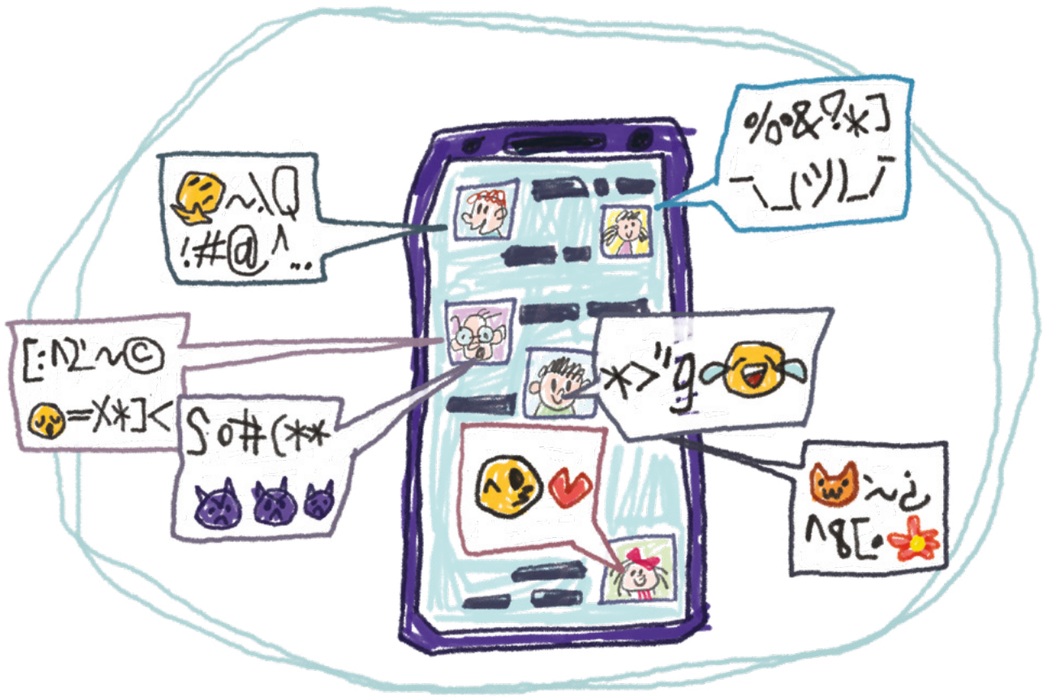


6 >> ЦИФРОВОЙ СЛЕД И БИОМЕТРИЧЕСКИЕ ДАННЫЕ

Цифровой след начинает накапливаться ребенком с самого раннего возраста. Это может являться вектором для разнообразных атак: неосторожное высказывание в интернете может стать поводом для увольнения, а обширный цифровой след, биометрические и персональные данные — цель для мошенников, сталкеров и других злоумышленников.

7 >> ТРАНСФОРМАЦИЯ СОЦИАЛЬНЫХ НАВЫКОВ ДЕТЕЙ

Дети стали больше общаться онлайн, пользоваться домашними устройствами с искусственным интеллектом и формировать парасоциальные связи с блогерами и инфлюенсерами. Процесс освоения социального поля изменился, и у детей могут появляться проблемы



с традиционной формой социализации. При этом риски, связанные с зависимостью от интернета, социальных сетей и компьютерных игр, будут находить все большее распространение.

8 >> ПОПУЛЯРИЗАЦИЯ «СЕРЫХ» ВЗАИМОДЕЙСТВИЙ

Массовые ограничения доступа к ресурсам в интернете и возможная регионализация интернета уже привели к распространению различных сервисов и подходов по преодолению вводимых запретов. Такие программы популярны и у взрослых, и у детей, имеют удобный интерфейс и часто выкладываются в интернет с руководствами по настройке. Популяризация «серых» взаимодействий может привести ребенка не только к изучению информационных технологий, но и вступлению в хакерскую ячейку на роль так называемого «script kiddie» — юного подмастерья более опытных хакеров.

9 >> УЖЕСТОЧЕНИЕ ИНФОРМАЦИОННОЙ ВОЙНЫ

Разные акторы все активнее используют киберпространство для информационных войн. Дети не обладают развитым критическим мышлением, поэтому наиболее уязвимы — они невольно оказываются главными жертвами информационных войн, последствия от которых будут множиться и становиться все менее предсказуемыми.

10 >> РОСТ ЦИФРОВОГО РАЗРЫВА

Цифровое неравенство и фактическое поражение в гражданских правах детей из отдельных стран может ограничить их в способности получить своевременную помощь и защиту: провайдеры услуг не смогут воспользоваться полным спектром мер по противодействию киберрискам, а правоохранительные органы будут ограничены в расследовании преступлений.

Рекомендации стейкхолдерам

4

>>

Проведенный анализ угроз и рисков, с которыми сталкиваются дети и подростки в процессе использования интернета, позволяет сформулировать ряд рекомендаций стейкхолдерам, в той или иной степени ответственным за реализацию технологий обеспечения безопасности в онлайн-среде.

К числу таких стейкхолдеров мы относим государство, образовательные учреждения, коммерческие предприятия, родителей, некоммерческие организации (НКО) и социальных предпринимателей, а также ИТ-разработчиков.

Важно учитывать, с одной стороны, что эффективная защита может быть достигнута при условии скоординированных и обоснованных усилий со стороны всех заинтересованных сторон. С другой стороны, мы убеждены, что ключевая роль в обеспечении интернет-безопасности заключается в содействии процессу формирования ребенка как осознанного и опытного субъекта, активно использующего цифровые ресурсы для своего развития.

Государство

Государство должно взять на себя ведущую роль по организации и координации совместной деятельности различных стейкхолдеров. Необходимо расширение поддержки существующих и создание новых коммуникационных площадок, предназначенных для обсуждения проблем кибербезопасности и поиска совместных путей их решения.

Необходимы государственные программы кодификации и мониторинга проблем кибербезопасности детей и подростков, а также программы поддержки междисциплинарных теоретических и прикладных исследований в данной сфере.

Законодательное регулирование персональных данных нуждается в совершенствовании в части открытости и безопасности практик, связанных с данными детей и подростков. Цифровые права детей как частных, так и платформенных пользователей должны быть пересмотрены и пересматриваться регулярно.

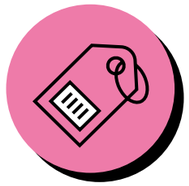
Образовательные учреждения

Перед образовательными учреждениями стоит комплексная задача, связанная одновременно с безопасным включением онлайн-технологий в учебный процесс, реализацией учебных программ и дисциплин, посвященных интернет-безопасности, а также цифровой социализацией детей и подростков. Необходимо проведение комплексного анализа киберрисков и стандартизация процессов, связанных с использованием компьютерных и интернет-технологий в образовании.

Образовательные модули по кибербезопасности и цифровой грамотности должны стать сквозным направлением в образовании детей и подростков на всех этапах обучения. Кроме того, должны быть разработаны программы повышения квалификации для специалистов, по роду деятельности связанных с киберзащитой детей и подростков (педагоги, юристы, сотрудники правоохранительных органов, психологи и т. д.).

Педагоги должны стать модераторами бытовой культуры безопасности использования интернета и цифровых технологий. Институт классного руководителя и школьного психолога нуждается в переосмыслении с учетом цифровизации среды, окружающей детей и подростков. Совместными усилиями педагогов и родителей необходимо находить баланс между контролем и приватностью, при этом основной задачей должна стать реализация интернет-потребностей и интересов школьника на основе взаимоуважения, поддержки и развития самостоятельности.

Коммерческие предприятия

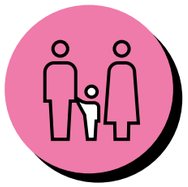


В целом, задача бизнеса в области обеспечения интернет-безопасности детей и подростков заключается в социально ответственной позиции по отношению к рискам и угрозам, возникающим по отношению к данной категории населения при разработке и реализации цифровых товаров и услуг, рассчитанных на различные целевые аудитории.

Коммерческие предприятия должны проводить этическую экспертизу распространяемого цифрового контента, элементов дизайна, пользовательских интерфейсов, внедряемых UX/UI решений и др. Соответствующий функционал должен входить в сферу ответственности специальных сотрудников, занимающихся вопросами соблюдения требований в области кибербезопасности детей и подростков («Chief Kids Compliance Officer»).

Особое внимание следует уделять разработке инициатив, направленных на поддержку и развитие сотрудничества бизнеса и других ключевых стейкхолдеров в области разработки и внедрения новых эффективных механизмов обеспечения приватности детей и подростков в онлайн-среде.

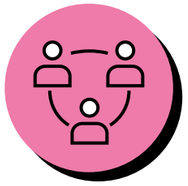
Родители



Родителям принадлежит ключевая роль в первичной социализации детей, организации их повседневных практик.

Во-первых, необходима вовлеченность родителей в виртуальную жизнь своих детей, проявление уважения и интереса к этой части социализации личности. Во-вторых, следует использовать все возможности для повышения собственных компетенций в области цифровой грамотности и кибербезопасности. В-третьих, необходимо делиться лучшими практиками организации интернет-активности детей, учитывающих баланс между их приватностью и контролем над действиями. И наконец, не стоит игнорировать доступные технологические инструменты информационной безопасности детей и подростков.

НКО



Задача общественных организаций, так или иначе связанных с проблемами интернет-безопасности детства, заключается в распространении инициатив, направленных на развитие данного направления, а также в координации действий различных факторов.

Функция НКО заключается в создании и поддержке междисциплинарных дискуссионных площадок по вопросам кибербезопасности детей и подростков. НКО способны выступать в качестве центров знаний и компетенции для различных стейкхолдеров, нуждающихся в соответствующей экспертизе.

Они также должны взять на себя адресную поддержку детей и подростков, столкнувшихся с последствиями различного типа кибератак, нуждающихся в реабилитации и ресоциализации. Следует отдельно отметить перспективность развития социального предпринимательства в сфере интернет-безопасности детей и подростков.

ИТ-разработчики

ИТ-разработчики являются источником профессиональных компетенций в области кибербезопасности, а также создателями продуктов, направленных на информационную защиту различных категорий населения, включая детей и подростков.

Эффективная деятельность по разработке ИТ-решений, поддерживающих кибербезопасность и снижающих риски пользователей интернета, невозможна без обмена опытом, дискуссий на профессиональных и индустриальных мероприятиях, в том числе международного уровня, изучения и использования зарубежного опыта, лучших практик.

Одним из наиболее перспективных направлений в данной области представляется развитие комплекса превентивных мер защиты на базе больших данных, профилирования, предиктивной аналитики и непрерывного мониторинга за счет сотрудничества со специалистами в области психологии, криминалистики и т. д.

Также следует обратить внимание на важность обеспечения экологичной разработки программных продуктов с учетом принципов и целей в области устойчивого развития ООН.

Методология

5

>>

Исследование
проводилось
в два этапа:

1. Анализ первичных
источников
2. Опрос экспертов

Первый этап

1 >> Был проведен кластерный анализ на основе выборки, включающей более 21 тысячи научных статей.

>21 000
научных статей

2 >> Были проанализированы более 500 источников литературы, посвященных теме безопасности несовершеннолетних в интернете.

>500
источников литературы

3 >> После первичной систематизации были выделены 23 киберриска. Объединение рисков в категории происходило на основе независимого экспертного кодирования: в работе участвовали 4 эксперта, каждый из которых создавал собственный набор категорий. После этого результаты работы каждого эксперта сравнивались с другими, и принималось решение о формировании категории и о ее названии. Расхождения обсуждались, и по каждому из них эксперты приходили к согласию.

23
киберриска

4 >> Для каждой категории мы сформировали описание, содержащее определение, рассказ о сути и специфике угрозы, доступную статистику и исследования, а также кейсы и примеры.

5 >> Мы проанализировали более 300 ИТ-решений, патентов, коммерческих компаний, платформ и сервисов с точки зрения их реальной или потенциальной способности противодействовать киберрискам. В результате по той же аналитической процедуре были сформированы 8 категорий ИТ-решений.

8
категорий ИТ-решений

Второй этап

Второй этап также строился на методологии агрегированных экспертных оценок. Цель этапа — рассортировать 23 киберриска по степени их опасности и эффективности технологических мер защиты детей от конкретного риска.

Для участия в работе были отобраны 24 эксперта — специалисты в области интернет-исследований (социологи, психологи, педагоги), кибербезопасности и ИТ-сферы. Каждому эксперту были предложены материалы — «карточки-паспортички» киберрисков и защитных ИТ-решений. Кроме того, был проведен онлайн-семинар с презентацией результатов первого этапа исследования, разбором киберрисков и заданий для экспертной работы.

>> КАЖДОМУ ЭКСПЕРТУ ПРЕДЛОЖИЛИ ОЦЕНИТЬ ПО 10-БАЛЛЬНОЙ ШКАЛЕ:

«Степень опасности» каждого риска: тяжесть последствий для психологического и физического здоровья ребенка, влияние на социальное благополучие, сложность реабилитации.

1 — риск не опасен
10 — риск имеет критический уровень опасности

«Эффективность технологий» защиты: насколько хорошо имеющиеся технологии защищают ребенка от конкретного киберриска.

1 — защиты нет / технологии не эффективны / их нет
10 — существующие технологии полностью защищают от риска

Полученные оценки для каждого из рисков и для каждой технологии были проанализированы на сходимость. Оценивались различные варианты средних оценок (средняя арифметическая, медиана), а также статистическая вариация. В результате были выявлены случаи бимодального распределения. В основном это касалось оценок эффективности информационных технологий. Бимодальное распределение указывает на значимое расхождение мнений: часть экспертов приписывали определенной технологии высокую способность защищать от рисков, а часть наоборот — приписывала более низкие оценки.

После завершения процедуры мы попросили некоторых экспертов прокомментировать их логику выставления оценок. Рассуждения и замечания систематизированы в отчете по результатам исследования.

Особенностью данного исследования является использование в его основе искусственного интеллекта (машинного обучения), превалирование методов автоматического количественного анализа в целях обеспечения достоверности результатов. Представленная информация и выводы получены с применением интеллектуальной аналитической системы выявления новых рынков, перспективных технологий и методов их использования TeqViser.

TeqViser — инструмент для объективного и своевременного принятия решений, который способен существенно дополнить традиционные методы оценки экономических перспектив инновационных разработок и технологических стартапов. Цифровые технологии не только существенно расширили исследуемую выборку, но и значительно сократили срок обработки исходных данных, представляя результаты и рекомендации для принятия управленческих решений. Исследование основано на анализе первичных источников, преимущественно текстовых англоязычных. Для получения структурированных данных из полученных массивов применяется машинный лингвистический анализ, а также анализ частоты упоминаний того или иного направления технологического развития и сферы его применения.

Внутренняя аналитика с использованием платформы TeqViser

Внешняя аналитика

Публикации в СМИ

Научный публикации

Анализ отчетов международных и консалтинговых компаний

TEQVISER

Кейсы технологий

Инвестиции

Патенты

Источниками данных для исследования служат накопленные за несколько лет базы данных, которые позволяют анализировать тренды на разных этапах жизненного цикла, начиная от решения фундаментальных научных проблем и заканчивая практическим применением технологий в рыночных продуктах и решениях. В качестве исходных данных выбраны первичные не интерпретированные экспертами свидетельства развития технологий.

Общая база TeqViser

1,2 млн
публикаций СМИ

608 000
инвестиций

33 млн
патентов

64 млн
научных публикаций

Риски в интернете

53 000
публикаций СМИ

2 200
инвестиций

32 000
патентов

109 000
научных публикаций

Риски для детей в интернете

13 000
публикаций СМИ

120
инвестиций

1 000
патентов

22 000
научных публикаций

Ручной анализ

500+
научных статей

200
патентов и решений

100
ИТ-компаний

Об авторах

>> БОРИС ГЛАЗКОВ

Вице-президент по стратегическим инициативам ПАО «Ростелеком»

>> ПАВЕЛ КРАСОВСКИЙ

Заместитель директора Центра стратегических инноваций ПАО «Ростелеком»

>> РУСЛАН ЮСУФОВ

Управляющий партнер MINDSMITH

>> МАКСИМ КОНДРАТЬЕВ

Аналитик, MINDSMITH

>> АНАСТАСИЯ ТЕТЕРКИНА

Аналитик, MINDSMITH

>> НАТАЛЬЯ КУРОВСКАЯ

Аналитик, MINDSMITH

>> ДАРЬЯ ВОРОНИНА

Старший аналитик, MINDSMITH

>> ИВАН КЛИМОВ

Эксперт MINDSMITH, доцент факультета социальных наук, старший научный сотрудник Международной лаборатории прикладного сетевого анализа НИУ ВШЭ

>> СЕРГЕЙ ДАВЫДОВ

Эксперт MINDSMITH, доцент Департамента социологии НИУ ВШЭ

>> ДАНИИЛ ЩЕРБАКОВ

Младший аналитик, MINDSMITH

>> МЫ ВЫРАЖАЕМ БЛАГОДАРНОСТЬ ЭКСПЕРТАМ

Алексею Гусеву
Анастасии Старковой
Артему Калашникову
Виктору Ивановскому
Денису Батранкову
Дмитрию Мананникову
Екатерине Легостаевой
Елизавете Паршиной
Кристине Рагузовой
Марии Зеленовой
Наталии Фельдман
Наталье Лезиной
Наталье Хилимончик
Оксане Демьяненко
Оксане Разумовой
Ольге Журавской
Ольге Игнатченко
Роману Шапиро
Рустэму Хайретдинову
Семёну Рожкову
Сергею Башук
Юлиане Чепурной

АЛЬЯНС ПО ЗАЩИТЕ ДЕТЕЙ В ЦИФРОВОЙ СРЕДЕ

Альянс по защите детей в цифровой среде — первое в России индустриальное объединение, направленное на создание дружелюбной, комфортной и безопасной для детей цифровой среды, способной в полной мере раскрыть творческий потенциал нового поколения. Альянс основали 1 сентября 2021 года девять крупнейших компаний России, работающих в сфере ИТ и коммуникаций: «ВымпелКом», «Газпром-Медиа Холдинг», «Лаборатория Касперского», «МегаФон», МТС, VK (ранее Mail.ru Group), «Национальная Медиа Группа», «Ростелеком» и «Яндекс».

Члены Альянса взяли на себя добровольные обязательства, призванные повышать цифровую грамотность детей, родителей и педагогов, развивать у детей навыки ответственного и безопасного поведения в интернете, демонстрировать им возможности созидательного использования цифровых технологий, формировать и продвигать позитивный и образовательный контент, разрабатывать новые подходы для защиты детей в интернете, создавать необходимые информационно-технологические решения для защиты личных данных, проактивно выявлять и удалять контент, который может причинить вред здоровью и развитию детей.

Важное направление работы Альянса — постоянный диалог с государством и международными организациями для объединения усилий по защите детей в цифровом мире. Альянс намерен стать лидером глобальной кооперации в сфере защиты детства в онлайн-среде и продвигать на международных площадках российские инициативы и подходы институтов гражданского общества, технологических- и медиакомпаний.

Подробная информация об Альянсе и его деятельности доступна на сайте: **https://internetforkids.ru**

«Технологии защиты
детей в интернете»

2022 год

ПАО «Ростелеком»
115172, Москва,
Гончарная ул., д. 30, стр. 1

Электронная почта:
rostelecom@rt.ru
Адрес для СМИ: pr@rt.ru

Тел.: +7(499) 999-82-83
Факс: +7(499) 999-82-22