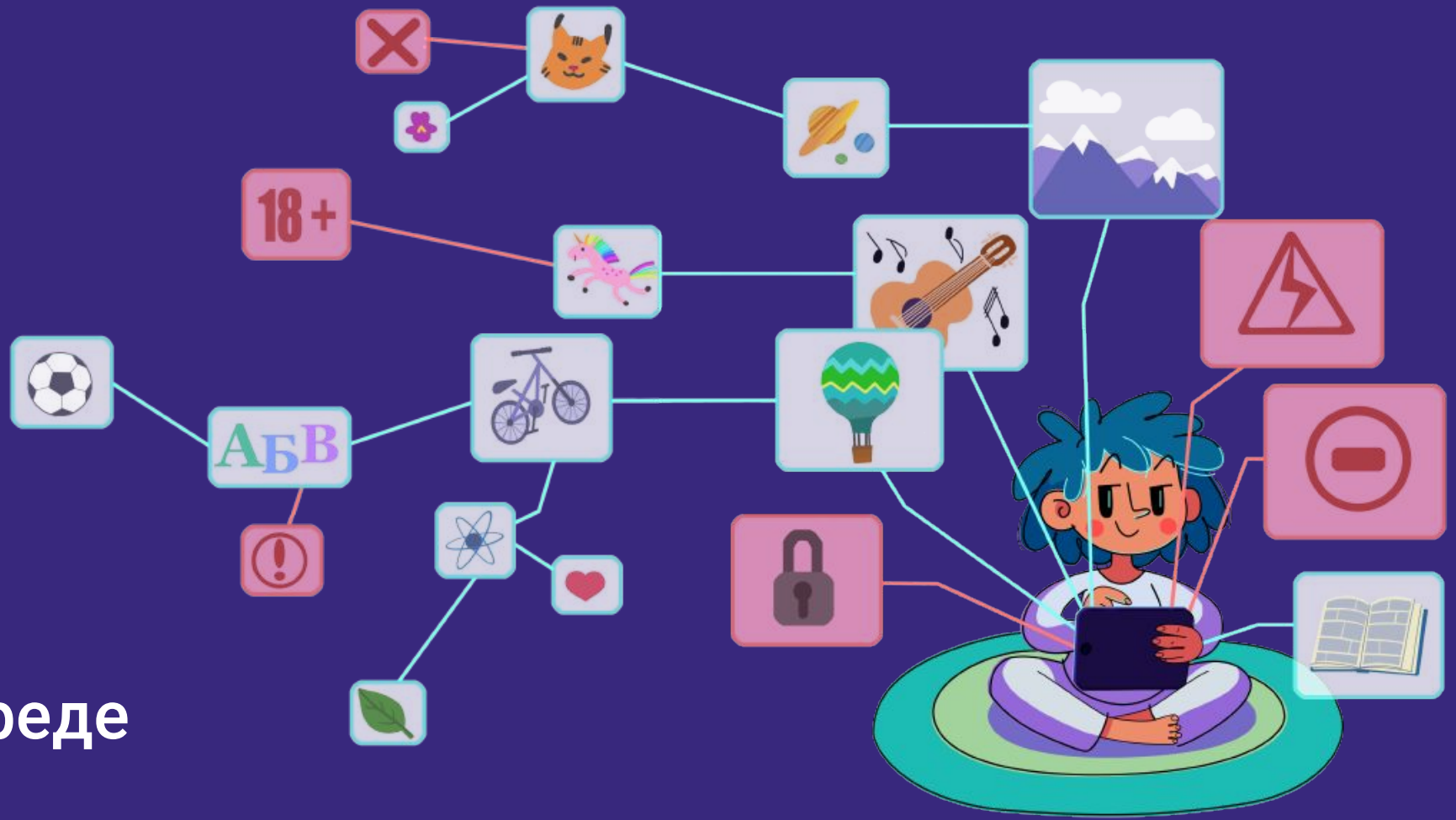
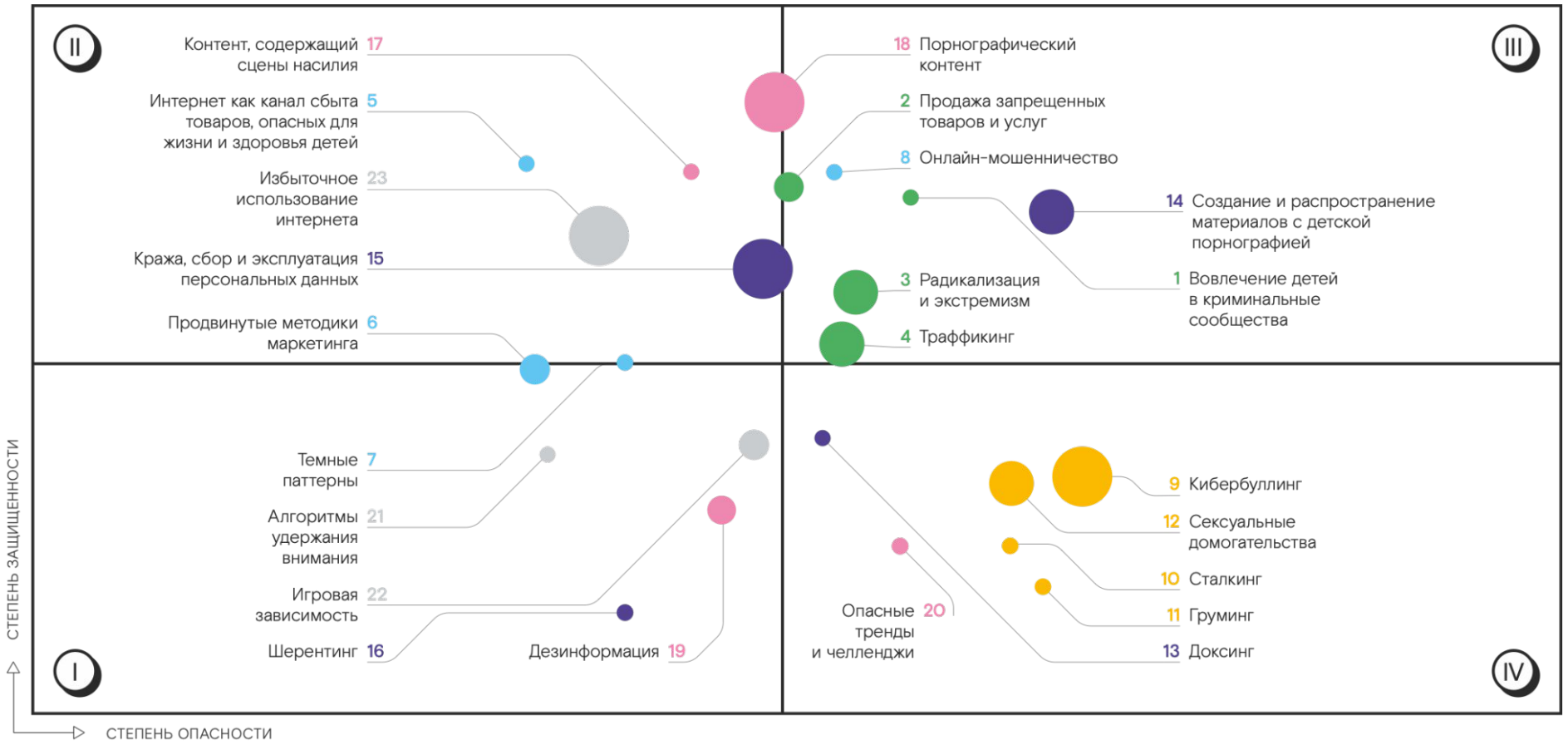
MINDSMITH



Киберриски в детской среде

MINDSMITH

карта рисков



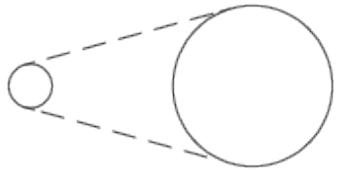
- Криминализация, втягивание в криминальные практики
- Маркетинговое давление, рискованные денежные отношения
- Личностная атака, психологическое насилие
- Цифровая эксплуатация, использование ребенка для создания цифрового контента
- Информационное давление, информация, не предназначенная для детей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

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



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

киберриски для детей и подростков

MINDSMITH

Криминализация, втягивание в криминальные практики

1. Вовлечение детей в криминальные сообщества
2. Продажа запрещенных услуг и товаров
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

MINDSMITH

киберриски для детей и подростков

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

MINDSMITH

Кластеры технологических решений

Было проанализировано 200+ решений и подходов, среди которых выделено 8 кластеров

MINDSMITH


Предиктивная аналитика
Детские социальные сети
Интернет-фильтры
Практики разработки
Сервисы оказания помощи
SOS
Инструменты родительского контроля и мониторинга
Инфраструктура
Автоматизированная модерация

MINDSMITH

» 1. 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.

Пример

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.

Его можно использовать как инструмент для определения опасных для детей сообществ.

MINDSMITH

» 2. 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.

Пример

GromSocial — детская социальная сеть, которая учит детей укреплять уверенность в себе 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.

» 3. 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.

MINDSMITH

Пример

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.

MINDSMITH

4. инструменты родительского контроля и мониторинга

Функционал инструментов родительского контроля направлен на проактивную регуляцию и мониторинг действий ребенка в интернете, поэтому такие программы позволяют выявлять и заблаговременно минимизировать киберриски для детей.

Пример

Kaspersky Safe Kids — российский сервис родительского контроля.

Совместим с Windows, macOS, Android и iOS, работает на всех устройствах.

В функционал входит: 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 ребенка по GPS.

MINDSMITH

» 5. интернет-фильтры

Интернет-фильтры 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.

Пример

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.

MINDSMITH

» 6. автоматизированная модерация

Модерация контента подразумевает удаление информации, ее фильтрацию или блокировку, рекомендацию контента через новостные ленты, тематические списки и персонализированные предложения, а также мониторинг контента.

Пример

Bullstop — мобильное приложение для предотвращения кибербуллинга в соцсетях.

Приложение определяет и фильтрует слова, выражения и от имени пользователя блокирует те контакты, которые постоянно отправляют сообщения, содержащие оскорбления, угрозы, тексты сексуального характера.

Входящие сообщения фильтруются и удаляются до того, как могли бы быть прочитаны, но сохраняются в архиве для последующего анализа.

Приложение также блокирует и отправку сообщений, включающих оскорбительный лексикон.

MINDSMITH

» 7. сервисы оказания помощи

Организации и сервисы, 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.

Пример

«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.

8. 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.

MINDSMITH

Пример

AviaTor — инфраструктурный проект INHOPE (международной ассоциации горячих линий интернета).

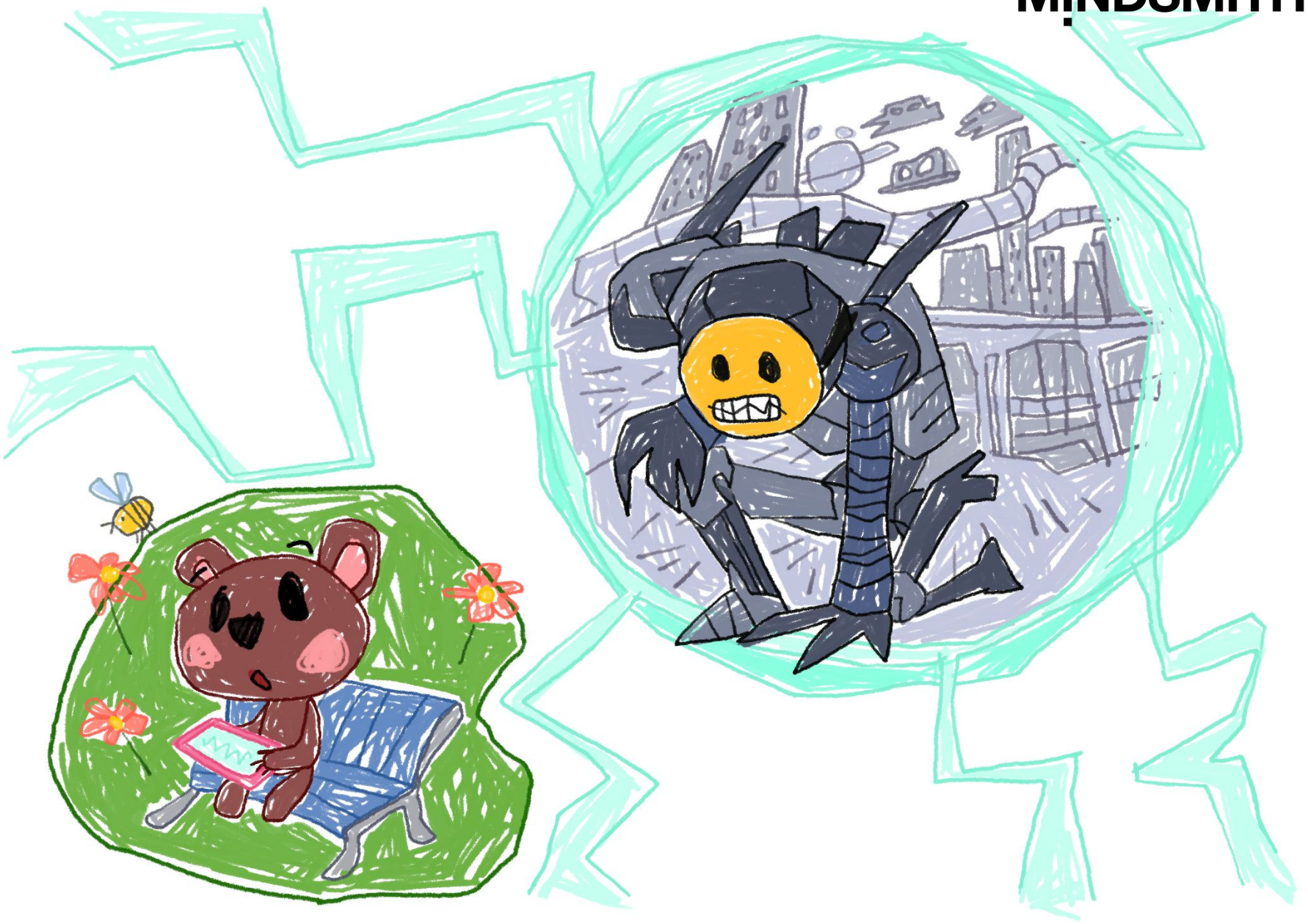
INHOPE объединяет 50 горячих линий в 46 странах для борьбы с материалами, содержащими сексуальное насилие над детьми. Организация ежегодно обрабатывает тысячи запросов.

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.

MINDSMITH

Риски в будущем

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.

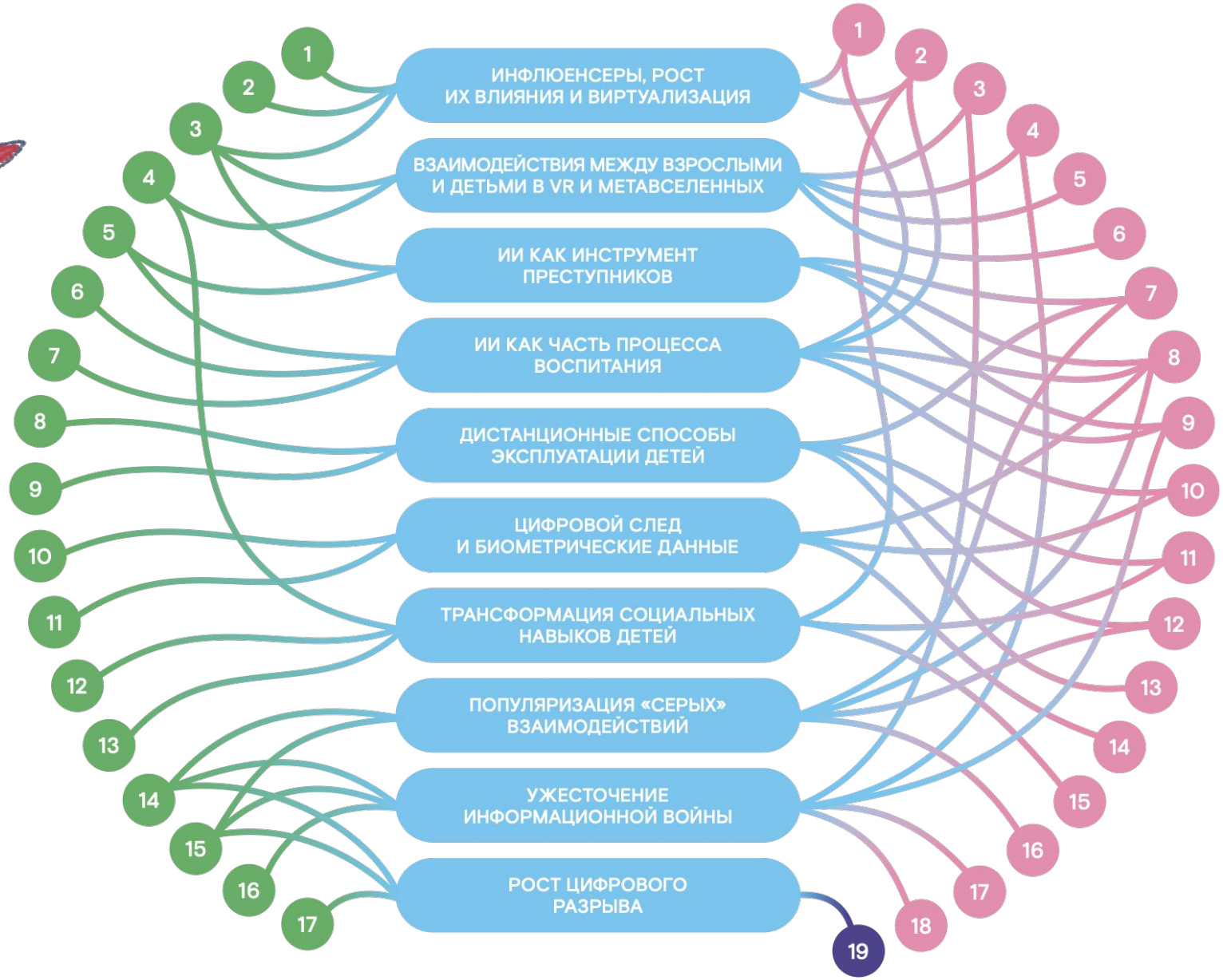


●Тренды и технологии

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



MINDSMITH

риски в будущем

1. Инфлюенсеры, рост их влияния и виртуализации

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.

MINDSMITH

риски в будущем

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.

MINDSMITH

риски в будущем

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.

риски в будущем

MINDSMITH

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.

риски в будущем

MINDSMITH

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.

MINDSMITH

Рекомендации стейкхолдерам

В числе стейкхолдеров: государство, образовательные учреждения, коммерческие предприятия, родители, некоммерческие организации (НКО) и социальные предприниматели, а также ИТ-разработчики.

рекомендации

MINDSMITH

Государство

- Организация и координация совместной деятельности стейкхолдеров
- Поддержка существующих и создание новых коммуникационных площадок
- Программы кодификации и мониторинга проблем кибербезопасности детей и подростков
- Программы поддержки междисциплинарных теоретических и прикладных исследований
- Совершенствование в части открытости и безопасности практик

Образовательные учреждения

- Модули по кибербезопасности в программы на всех этапах обучения
- Программы повышения квалификации
- Педагоги как модераторы бытовой культуры безопасности использования интернета и цифровых технологий
- Переосмысление института классного руководителя и школьного психолога
- Обучение и консультации родителей по вопросам кибербезопасности

рекомендации

MINDSMITH

Родители

- Вовлеченность родителей в виртуальную жизнь своих детей
- Непрерывное повышение собственных компетенций в области кибербезопасности и цифровой грамотности
- Выработка лучших практик по установлению баланса между приватностью ребенка и его безопасностью
- Использование существующих решений для минимизации киберрисков

Коммерческие предприятия

- Социально ответственная позиция по отношению к кибербезопасности детей
- Этическая экспертиза распространяемого цифрового контента, элементов дизайна, пользовательских интерфейсов и пр.
- Назначение человека, ответственного за безопасность детей и подростков («Chief Kids Compliance Officer»)
- Поддержка и развитие сотрудничества бизнеса и других стейкхолдеров в области разработки и внедрения эффективных механизмов защиты

рекомендации

MINDSMITH

НКО

- Распространение инициатив, направленных на развитие направления по защите детей и подростков в интернете
- Центры знаний и компетенции для различных стейкхолдеров, нуждающихся в соответствующей экспертизе
- Создание и поддержка междисциплинарных дискуссионных площадок
- Адресная поддержка детей и подростков, столкнувшихся с последствиями различного типа кибератак
- Развитие социального предпринимательства

ИТ-разработчики

- Разработка ИТ-решений, поддерживающих кибербезопасность и снижающих киберриски
- Обмен опытом, дискуссии на профессиональных и индустриальных мероприятиях
- Изучение и использование зарубежного опыта, лучших практик
- Развитие комплекса превентивных мер защиты на базе больших данных и профилирования за счет сотрудничества со специалистами в области психологии, криминалистики
- Обеспечение экологичной разработки продуктов с учетом принципов и целей в области устойчивого развития ООН

MINDSMITH

Узнайте больше о защите детей в интернете

Ростелеком

АЛЬЯНС ПО ЗАЩИТЕ ДЕТЕЙ В ЦИФРОВОЙ СРЕДЕ

TEQVISER

MINDSMITH

Пройдите тестирование и получите сертификат

Ростелеком

АЛЬЯНС ПО ЗАЩИТЕ ДЕТЕЙ В ЦИФРОВОЙ СРЕДЕ

TEQVISER

MINDSMITH

Спасибо за ваше время!

@YUSUFOVRUSLAN

Руслан Юсуфов

Управляющий партнер
MINDSMITH

yusufov@mindsmith.ru