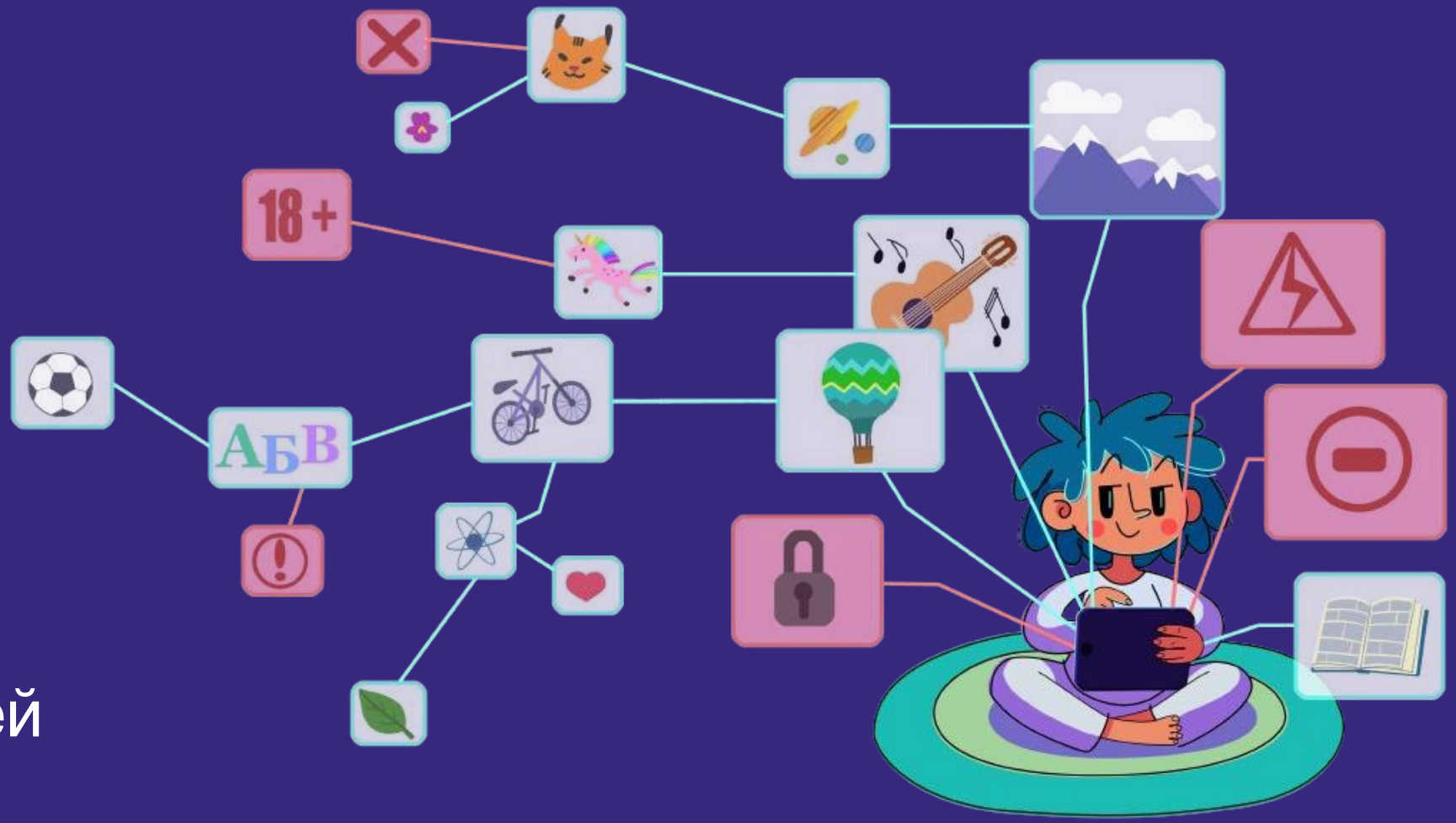
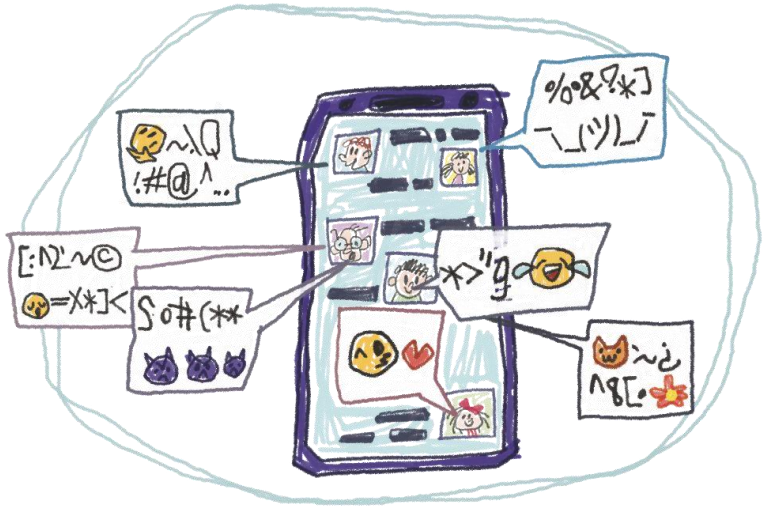
АЛЬЯНС
ПО ЗАЩИТЕ ДЕТЕЙ
В ЦИФРОВОЙ СРЕДЕ




# Технологии защиты детей в интернете

Ростелеком MINDSMITH TEQVISER

# Дети активно пользуются интернетом



**80 %**

детей в возрасте от 3 до 14 лет пользуются интернетом хотя бы раз в день

Источник: Росстат, 2020

**68,3 %**

детей в возрасте от 3 до 6 лет активно пользуются интернетом

Источник: НИУ ВШЭ, 2022

**50 %**

детей и подростков публично раскрывают свой возраст и выкладывают личные фотографии в социальных сетях

Источник: «Лаборатория Касперского», 2021

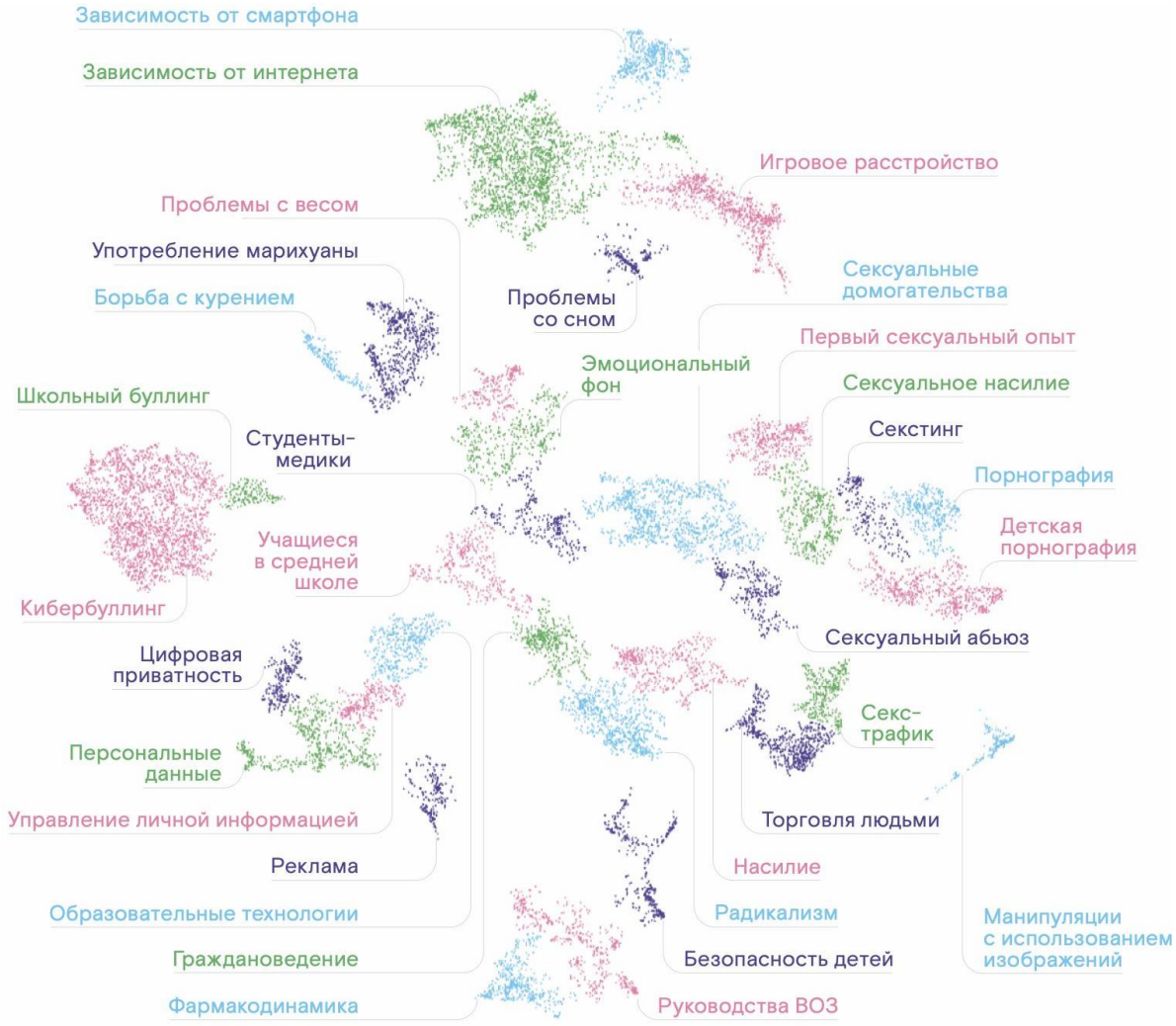
# Как проводилось исследование

1. Кластерный анализ на основе выборки, включающей более 21 тыс. научных статей. В результате было выделено 33 кластера рисков.

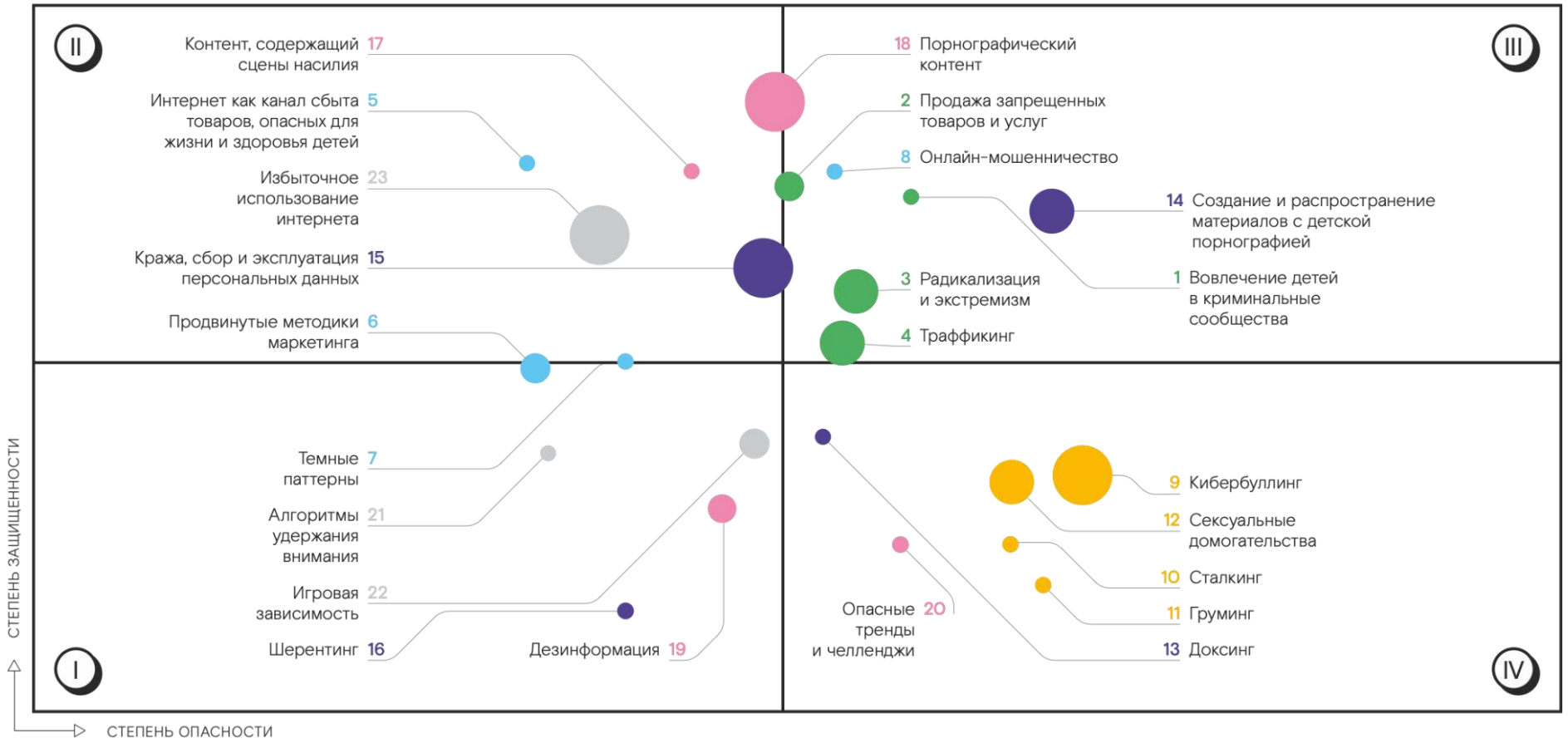
2. Анализ 500+ источников литературы, по результатам которого было выявлено 23 киберриска, угрожающих безопасности детей и подростков.

3. Анализ 300+ патентов, компаний и ИТ-решений в области кибербезопасности детей. Сформировано 8 кластеров технологических решений.

4. Опрос экспертов в области кибербезопасности, детской психологии и социологии для определения степени опасности рисков и защищенности от них.



# Карта рисков



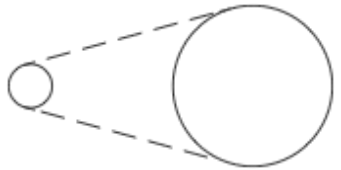

- Криминализация, втягивание в криминальные практики
- Маркетинговое давление, рискованные денежные отношения
- Личностная атака, психологическое насилие
- Цифровая эксплуатация, использование ребенка для создания цифрового контента
- Информационное давление, информация, не предназначенная для детей 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).

# Риски, требующие внимания

## Опасные тренды и челленджи

#TidePodChallenge — глотание на камеру капсул для стирки (компактные капсулы с моющим веществом похожи на конфеты).

Во время челленджа центры токсикологического контроля получили сообщения о более чем 10 500 случаях отравления подобными веществами детьми от 5 лет и младше.

## Сталкинг

Мужчину обвинили в сталкинге и сексуальных домогательствах после того, как он нашел место жительства японской певицы по отражению здания в ее зрачках на селфи.

Он также использовал Google Street View, изучил все видео и фотографии в соцсетях, узнав информацию вплоть до расположения штор и направления естественного света, чтобы определить, где именно находится ее квартира.

# Криминализация, втягивание в криминальные практики

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

# Кластеры технологиче ки решений

# Кластеры технологических решений

Предиктивная аналитика — позволяет прогнозировать и выявлять риски на ранней стадии.

PrevBOT — чат-бот, определяющий опасные паттерны поведения в переписках.

Детские социальные сети — соцсети только для детской аудитории с дополнительными функциями фильтрации и модерации.

GromSocial — детская социальная сеть.

Практики разработки — создание и улучшение функционала, касающегося детской безопасности.

Deutsche Bank API Program — решение для проверки возраста для доступа к сайту.

Инструменты родительского контроля и мониторинга — проактивная регуляция и мониторинг действий ребенка в интернете.

Kaspersky Safe Kids — российский сервис родительского контроля.

Интернет-фильтры — фильтрация интернет-ресурсов по темам и ключевым словам.

Lidrekon — расширение для браузера, позволяющее фильтровать контент.

Автоматизированная модерация — мониторинг, удаление, фильтрация и / или блокировка контента.

Bullstop — мобильное приложение для предотвращения кибербуллинга в соцсетях.

Сервисы оказания помощи — сервисы, которые позволяют запросить помощь специалистов.

«Трудно подросткам» — чат-бот для детей, пострадавших от травли.

Инфраструктура — совокупность решений в области безопасности, интегрированных в единую систему.

AviaTor — инфраструктурный проект INHOPE, позволяющий маркировать вредоносный контент и блокировать подобные материалы.

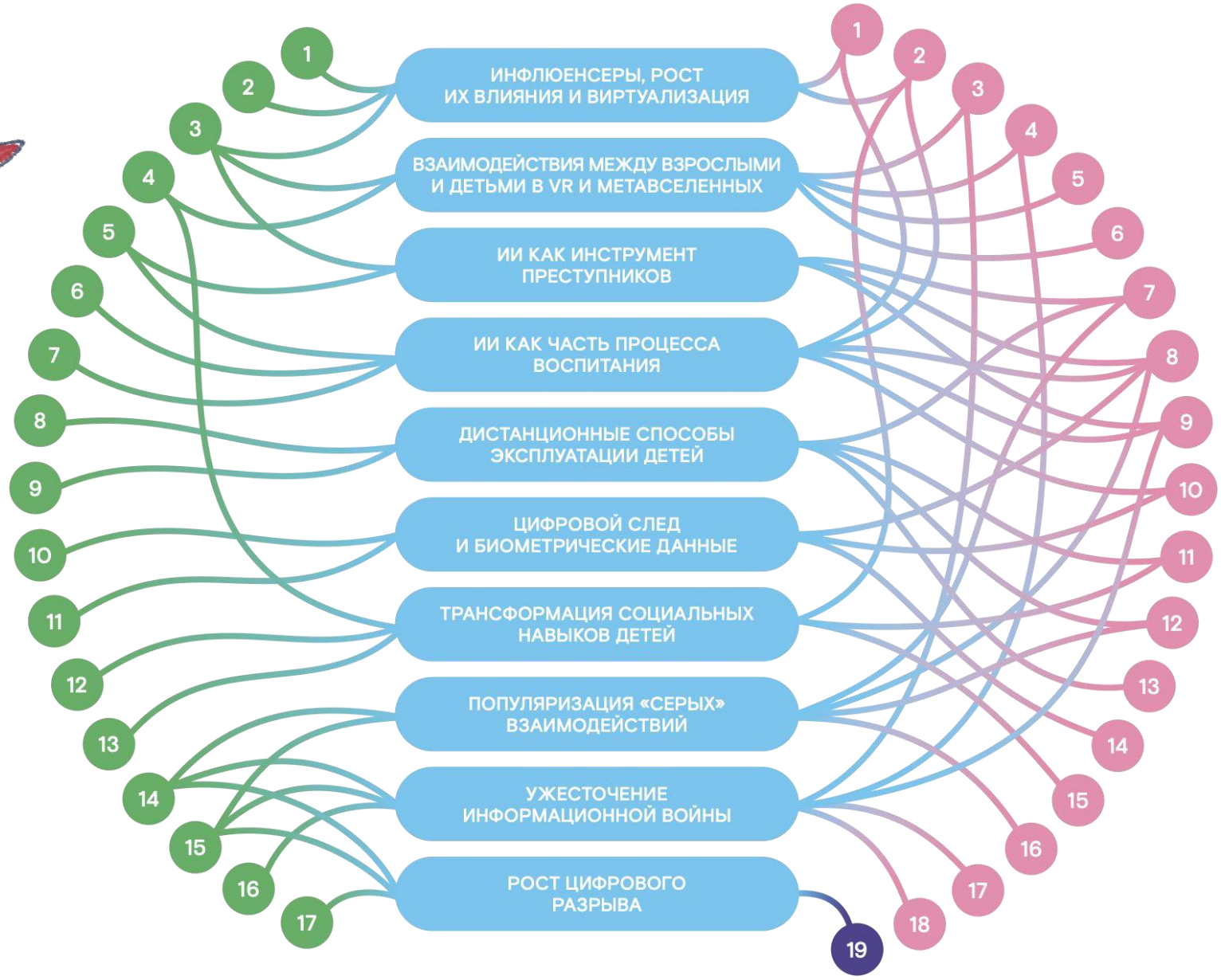
# Риски в будущем

● 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

18. Опасные тренды и челленджи
19. Алгоритмы удержания внимания
20. Кибербуллинг
21. Сталкинг
22. Груминг
23. Сексуальные домогательства
24. Онлайн-мошенничество
25. Кража, сбор и эксплуатация персональных данных
26. Дезинформация
27. Продвинутые методики маркетинга
28. Игровая зависимость
29. Продажа запрещенных товаров и услуг
30. Темные паттерны
31. Шерентинг
32. Избыточное использование интернета
33. Вовлечение детей в криминальные сообщества
34. Доксинг
35. Радикализация и экстремизм
36. Включает все 23 риска



MINDSMITH

## ИИ как часть процесса воспитания

Существует вероятность, что дети, пользующиеся ИИ-ассистентами как игрушками, станут жертвами создателей таких приборов.

Создатели могут транслировать через них идеи, манипулировать алгоритмами подбора контента, собирать данные.

Пример

Сервис Alexa, встроенный в умную колонку Amazon Echo, порекомендовал десятилетней девочке опасный и потенциально смертельный способ развлечься.

Девочка попросила голосового помощника подыскать ей самый популярный челлендж. «Задача проста: вставьте зарядное устройство для телефона в розетку примерно наполовину, а затем приложите монетку к открытым контактам», — порекомендовала Alexa.

Данный челлендж стартовал в TikTok и набрал популярность в сети. Вовлекая всё больше детей, он был назван «ночным кошмаром школ».

# Рекомендации стейкхолдерам

# Рекомендации

Государство

- Поддержка существующих и создание новых коммуникационных площадок для совместной деятельности стейкхолдеров
- Программы кодификации и мониторинга киберрисков, совершенствование в части открытости и безопасности практик

Родители

- Непрерывное повышение собственных компетенций в области кибербезопасности
- Установление баланса между приватностью ребенка и контролем за его безопасностью

Образование

- Модули по кибербезопасности на всех этапах обучения, программы для преподавателей и родителей
- Переосмысление института классного руководителя и школьного психолога

ИТ-компании

- Источник профессиональных компетенций в области кибербезопасности
- Изучение лучших практик и обмен опытом, дискуссии на профессиональных и индустриальных мероприятиях

Коммерческие предприятия

- Этическая экспертиза распространяемого цифрового контента, элементов дизайна, пользовательских интерфейсов
- Назначение ответственного человека за безопасность детей и подростков

НКО

- Распространение инициатив, направленных на развитие направления по защите детей и подростков в интернете
- Адресная поддержка детей и подростков, столкнувшихся с последствиями кибератак