1. **Как задать ребенку вопрос, есть ли какие-то бедовые проникновения в его (ее) жизнь? И если все пользуются ИИ для создания негативного контента, нельзя сделать зеркальный ответ, в виде тех же фильтров которые обрабатывают информацию от социальных платформ?**

   Нужно строить доверительные отношения с ребенком. Сами генеративные инструменты на базе ИИ обычно имеют слои и модули для фильтрации нежелательных запросов. Сами соцсети и приложения для защиты детей имеют встроенные фильтры, базирующиеся на ИИ. Но это не является универсальным решением, так как если ребенок захочет, он найдет вредный контент: попросит у сверстника смартфон, изменит настройки приложения для защиты, заведет аккаунт без детских настроек. Ребенку нужно объяснять, зачем и почему такие приложения устанавливаются на его устройства.

2. **Как родители могут контролировать цифровую свободу ребенка? Что предпринять взрослым для защиты детей от киберугроз?**

   Существует широкий инструментарий, но он все равно не сможет защитить ребенка в 100% случаев. Кроме того, полная защита от всех угроз приведет к появлению взрослого человека, который с этими угрозами никогда не сталкивался. Задачей родителя должен быть не тотальный контроль деятельности ребенка в сети, а его сопровождение, воспитание и обучение.

3. **Рассматриваете ли вы угрозу распространения клипового мышления как один из актуальных рисков?**

   Клиповое мышление является следствием использования корпорациями темных паттернов, а не самостоятельной угрозой. Мозг детей обладает крайне высокой нейропластичностью, поэтому они быстро и легко приспосабливаются к интерфейсам, форматам контента и другим специфичным особенностям потребления информации в сети.
   Короткий контент, подающийся бесконечным потоком и не требующий рефлексии, который приводит к усилению клипового мышления у ребенка, относится к темным паттернам.

4. **Как меняются особенности киберугроз в зависимости от региона РФ? Как сказываются региональные особенности на характере уже реализованных угроз?**

   Кажется, на тему особенностей изменения киберугроз в зависимости от регионов РФ можно написать не одну диссертацию, так как разные регионы сильно различаются в нюансах культуры, демографии, социальной защищенности, экономической активности и т.д. В целом, описанные угрозы универсальны, но конкретные случаи реализации рисков будут приобретать региональную специфику и изменяться в статистических параметрах в зависимости от вышеобозначенных факторов.

Хорошим аналогом здесь будет разница киберрисков и специфики их реализации по миру. Так, в Латинской Америке крайне остро стоит проблема вербовки подростков в криминальные сообщества, а в Юго-Восточной Азии статистически чаще происходят похищения и сексуальная эксплуатация. Корнем таких различий являются разница в социальных, экономических и культурных особенностях регионов.

5. **Многие приведенные примеры касаются иностранной аудитории, условно говоря, не наших детей. Означает ли это, что у нас ситуация в этой группе киберрисков лучше? Или просто у нас ситуация в группе киберрисков для подростков просто не до конца исследована?**

   Эмпирически — сильно зависит от рисков. Какие-то из них у нас и правда куда чаще реализуются, а какие-то реже, чем, например, на западе или в Китае. Тезис о том, что ситуация по киберрискам для детей в России не до конца исследована, верен. Во-первых, верен он потому, что киберриски техногенны по своей природе. То есть с появлением новых технологий и новых бизнес-моделей, как легальных, так и криминальных, которые этими технологиями драйвятся, придется проводить новые и новые исследования. Во-вторых, высокая степень проникновения интернета — недавний феномен. Двадцать лет назад интернетом не пользовалось такого количества людей всех возрастов и бэкграундов. Из-за этого влияние многих механик, например, рекомендательных алгоритмов, на детей не исследовано в полной мере по всему миру.

6. **Случай из жизни - подросток с паспортом начал играть в онлайн-казино, набрал для этого микрозаймов на паспорт более 400 тыс. Прошел по рекламной ссылке. Как защитить от этого?**

   Существуют приложения, позволяющие отслеживать онлайн-активность ребенка и обсуждать с ним его деятельность в интернете. Кроме того, важно давать ребенку хотя бы базовое понимание правил финансовой грамотности. Знания в медиаграмотности и цифровой гигиене также значительно снижают вероятность, с которой ребенок окажется в такой или похожей ситуации.
   В случае наступления риска также стоит обратиться в правоохранительные органы и к юристу.

7. **А насколько эффективны детские аккаунты? Дети быстро научатся отключать эту функцию... В онлайн-кинотеатре, например.**

   Зависит от возраста и ребенка, но целиком доверять детскому аккаунту нельзя: так, встречаются случаи, когда контент, публикуемый на детских секциях платформ не курируется людьми, а определяется алгоритмом или создателями. В таких случаях злоумышленники могут производить крайне странный контент, смысл которого вполне себе взрослый, но алгоритмом считывается, как пригодный для детского потребления. Существуют также детские соцсети. Но сами дети ими пользоваться особо не хотят, а концепция соцсети

«исключительно для детей» привлекает злоумышленников, чьей целью дети являются.

Несовершеннолетние и правда быстро учатся отключать все фильтры и блокировки, поэтому детские аккаунты работают до тех пор, пока ребенок согласен ими пользоваться. Привести ребенка к выводу о том, что ему лучше использовать детский аккаунт — задача родителя и окружающих его взрослых.

8. **В России ведь нет детских соцсетей?**

   В России есть несколько проектов, связанных с детскими социальными сетями, но они имеют ряд ограничений. Многие проекты, которые запускались ранее, закрылись либо из-за низкой популярности, либо из-за того, что стандартный подход к монетизации в случае с детскими соцсетями вызывает ряд этических вопросов.

9. **Почему на уровне провайдера нельзя устанавливать кластеры защиты? чтобы перманентно блокировать сайты, соцсети мошенников. и запускать чат-ботов, которые будут все отслеживать?**

   Даже комбинации инструментов не позволят обезопасить детей, если окружающие их взрослые не учат их пользоваться интернетом. Кроме того, рано или поздно эти дети вырастут и начнут пользоваться взрослым интернетом, никогда ранее не столкнувшись с рисками и их последствиями. Последствия такого резкого скачка рисков могут быть крайне плачевными.

   Также, сайты с нежелательным для детей контентом, мошенники и прочие подобные вещи не стоят на месте. По сути, между стейкхолдерами и злоумышленниками происходит постоянная гонка в разработке новых методов и технических решений. Когда корпорация или правительство блокирует один сайт, злоумышленники могут открыть новый или создать «зеркало», которое позволяет попадать на сайт, обходя черный список. В связи с развитием генеративного ИИ и внедрением других технологий, тотальная слежка и фильтрация начнут занимать все больше и больше ресурсов, а также будут становиться экспоненциально сложнее и затратнее. В результате, каждый раз, когда злоумышленники будут находить новую брешь в защитах, существенная доля детей будет подвержена рискам, пока стейкхолдеры разрабатывают решение. Некоторые угрозы будут значительно меняться со временем — в условиях повального внедрения ИИ и прихода расширенной реальности, многие риски изменятся. Расширенная реальность позволит людям взаимодействовать друг с другом в киберпространстве на более глубоком уровне погружения, в связи с чем появится новый слой у каждого из рисков.

10. **Безопасно ли оставлять ребенка с Яндекс Алисой или Марусей наедине сегодня? Как их настроить правильно?**

    Оставлять ребенка полностью наедине с голосовыми ассистентами не опасно, если установлен детский режим. При этом важно подумать о том, насколько

здоровое восприятие сформируется у ребенка, если его досуг перекладывать на робота. Особенно это касается дошкольников и учеников начальной школы.

11. **Ваше мнение, стоит ли оставлять свою биометрию?**

    По возможности, лишние данные оставлять вообще нежелательно. Утечки данных происходят с пугающей регулярностью, при этом биометрия — тот вид данных, который поменять либо сложно, либо вообще невозможно. Разные учреждения по-разному хранят биометрию, у них различается зрелость кибербезопасности. Так, вероятность того, что биометрию вашу или вашего ребенка украдут у крупного банка значительно ниже, чем вероятность кражи биометрии у региональной сети пиццерий. Перед тем, как передать биометрические данные той или иной организации, стоит проверить, как часто у нее происходят утечки, насколько она крупная, и насколько хорошо у нее работают системы информационной безопасности.

12. **Чат-бот: а это не нарушает тайну переписки? Каким образом он читает чужие переписки?**

    Бот заходит в чат-комнаты, где присутствуют дети и ведутся дискуссии на взрослые темы. Технически, сделать то же самое может любой человек — чат-бот просто умеет их искать и работает быстрее.

13. **А если привязывать аккаунт на телефоне ребенка к своей почте? Тогда все уведомления можно настроить и контент в том числе, нет?**

    Ребенок может выйти из аккаунта или перепривязать его к новой почте. Продвинутый подросток может вовсе запустить другую операционную систему или иным образом выходить за пределы намеченных родителями границ, оставляя минимум следов.