

Проблемное поле (проблема)	Итоговые тезисы (способ/подход к решению)
1. ВВУИО+20. ГЛОБАЛЬНЫЙ ЦИФРОВОЙ ДИАЛОГ: ОТ СЛОВ К ДЕЛУ	
<p>1. Платформенная фрагментация и кризис согласованных правил</p> <p>Фрагментация подходов к регулированию цифровых платформ, различия между государственными и платформенными интересами, непрозрачность алгоритмов, манипулятивные интерфейсы и отсутствие единых процедур модерации препятствуют формированию согласованных правил цифрового управления и подрывают доверие к платформенной среде.</p> <p><i>Пункты проблем из полной версии тезисов: 1–7</i></p>	<p>1. Согласованная архитектура платформенного регулирования</p> <p>Необходим переход к согласованной модели регулирования платформ, включающей международные принципы платформенного управления, стандарты прозрачности алгоритмов и интерфейсов, независимый аудит, многосторонние механизмы согласования позиций государств и цифровых платформ, а также единые процессуальные стандарты модерации контента и обжалования решений об его удалении.</p> <p><i>Пункты подходов к решению из полной версии тезисов: 1–7</i></p>
<p>2. Разрыв между декларациями и имплементацией</p> <p>Согласованные на глобальном уровне цифровые принципы нередко сохраняют декларативный характер, не переходят в сопоставимые национальные меры и не обеспечивают измеримого прогресса, что снижает результативность международного цифрового диалога.</p> <p><i>Пункты проблем из полной версии тезисов: 8–9.1</i></p>	<p>2. Переход к модели исполнимых цифровых обязательств</p> <p>Следует перейти от декларативного формата к механизму обязательств с измеримыми результатами, сочетающему правовые и нормативно-технические инструменты, сопоставимые показатели, модельные пакеты имплементации, пилотные проекты, публичную отчетность и механизмы верификации прогресса.</p> <p><i>Пункты подходов к решению из полной версии тезисов: 8–9.1</i></p>
<p>3. Цифровая дилемма безопасности и дефицит кооперации</p> <p>Практика трансграничного воздействия в информационном пространстве, отсутствие единых процедур обмена информацией о киберинцидентах и различия в интерпретации цифрового суверенитета усиливают недоверие между государствами, повышают риски эскалации и затрудняют выработку устойчивых механизмов международного взаимодействия.</p> <p><i>Пункты проблем из полной версии тезисов: 10–10.1</i></p>	<p>3. Суверенно-кооперативная модель киберустойчивости</p> <p>Требуется выстраивание системы международного взаимодействия в сфере информационной безопасности на основе уважения суверенитета, включающей обмен информацией о киберинцидентах, универсальные рамки сотрудничества, двусторонние и многосторонние соглашения, инструменты развития киберпотенциала и совместные механизмы мониторинга и реагирования.</p> <p><i>Пункты подходов к решению из полной версии тезисов: 10–10.5</i></p>

<p>4. Суверенитет, неравенство и устойчивость цифрового развития</p> <p>Противоречие между цифровым суверенитетом и открытостью сети, неопределенность юрисдикции в трансграничных системах, ограничительные меры в отношении новых медиа, инфраструктурные дисбалансы, цифровое неравенство, зависимость развивающихся стран и дефицит доверия к цифровой среде затрудняют формирование справедливой и устойчивой модели глобального цифрового развития.</p> <p><i>Пункты проблем из полной версии тезисов: 11–29</i></p>	<p>4. Комплексная модель суверенной открытости и инклюзивного развития</p> <p>Необходима комплексная модель суверенной открытости и устойчивого цифрового развития, сочетающая стандарты интероперабельности, рамки разграничения юрисдикции, сбалансированное регулирование новых медиа, развитие инфраструктуры и сетевой нейтральности, сокращение цифрового разрыва, поддержку технологического суверенитета, финансирование цифровой трансформации, укрепление доверия, человеческого капитала, экологической устойчивости и правового режима цифрового наследия.</p> <p><i>Пункты подходов к решению из полной версии тезисов: 11–29</i></p>
<p>2. ПРАВОВОЙ ЛАНДШАФТ В ОБЛАСТИ ГЕНЕРАТИВНОГО ИИ</p>	
<p>1. Нормативная неопределенность генеративного ИИ</p> <p>Отсутствие унифицированного определения генеративного ИИ, отставание регулирования от темпов технологического развития, несогласованность международных подходов и искусственное противопоставление безопасности и инноваций создают правовую неопределенность и усиливают регуляторную фрагментацию.</p> <p><i>Пункты проблем из полной версии тезисов: 1–4</i></p>	<p>1. Рамочная и адаптивная модель регулирования</p> <p>Необходимо закрепить единое определение генеративного ИИ и сформировать рамочную адаптивную модель регулирования, сочетающую базовые правовые принципы, технологически нейтральные требования, регулярный пересмотр стандартов, меры поддержки отрасли и международные механизмы взаимного признания и координации.</p> <p><i>Пункты подходов к решению из полной версии тезисов: 1–4</i></p>
<p>2. Непрозрачность моделей и дефицит подотчетности</p> <p>Низкая прозрачность генеративных моделей, слабость механизмов независимого контроля и рост синтетического, манипулятивного и вредоносного контента подрывают доверие к информационной среде, затрудняют оценку надежности систем и повышают общественные риски.</p> <p><i>Пункты проблем из полной версии тезисов: 5–8</i></p>	<p>2. Прозрачность, аудит и превентивный контроль</p> <p>Следует ввести обязательные требования к прозрачности моделей, независимый аудит, многосторонний надзор, ограничение опасных сценариев использования, маркировку генеративного контента, оценку воздействия высокорисковых систем и обязательную экспертизу их влияния на права человека.</p> <p><i>Пункты подходов к решению из полной версии тезисов: 5–8</i></p>

<p>3. Кризис классических моделей юридической ответственности</p> <p>Классические конструкции юридической ответственности не учитывают автономный и вероятностный характер генеративных систем, что затрудняет распределение рисков, установление причинно-следственной связи и определение обязанностей участников жизненного цикла ИИ.</p> <p><i>Пункты проблем из полной версии тезисов: 9–11</i></p>	<p>3. Распределенная ответственность и алгоритмический риск</p> <p>Необходима модель распределенной ответственности и алгоритмического риска, при которой обязанности и меры ответственности распределяются между разработчиками, поставщиками и пользователями в зависимости от контроля, этапа жизненного цикла и уровня риска, при сохранении приоритета базовых правовых принципов и человеческого контроля.</p> <p><i>Пункты подходов к решению из полной версии тезисов: 9–11</i></p>
<p>4. Данные, предвзятость и уязвимость прав субъектов</p> <p>Отсутствие единых стандартов качества и репрезентативности данных, использование персональных данных без достаточных гарантий, а также диспропорции в обучающих выборках создают риски предвзятости, дискриминации, нарушения приватности и когнитивного доминирования ограниченного круга установок.</p> <p><i>Пункты проблем из полной версии тезисов: 12–13</i></p>	<p>4. Правовой режим качественных и защищенных данных</p> <p>Следует сформировать многоуровневую систему регулирования данных для ИИ, включая паспортизацию и аудит выборок, стандарты репрезентативности и контроля предвзятости, развитие локальных и культурно чувствительных наборов данных, а также четкие правовые основания и гарантии защиты персональных данных при обучении и применении моделей.</p> <p><i>Пункты подходов к решению из полной версии тезисов: 12–13</i></p>
<p>3. РОЛЬ ЦИФРОВОЙ МЕДИЙНОЙ РЕКЛАМЫ ДЛЯ БИЗНЕСА</p>	
<p>1. Перенасыщение рекламы и эрозия внимания аудитории</p> <p>Избыточный объем цифровой медийной рекламы снижает ее эффективность как инструмента формирования спроса, усиливает конкуренцию за внимание, провоцирует отток аудитории к альтернативным площадкам и ослабляет лояльность потребителей.</p> <p><i>Пункты проблем из полной версии тезисов: 1–2, 15, 17</i></p>	<p>1. Управляемая и стратегическая рекламная коммуникация</p> <p>Необходим переход от количественного наращивания рекламы к стратегическому управлению рекламным воздействием: саморегулирование объема и качества рекламы, развитие долгосрочных моделей коммуникации с потребителем, непрерывная аналитика и учет не только узнаваемости бренда, но и изменения восприятия потребностей аудитории.</p> <p><i>Пункты подходов к решению из полной версии тезисов: 1–2, 15, 17</i></p>

<p>2. Платформенная зависимость и регуляторные ограничения</p> <p>Государственные ограничения и доминирование крупных транснациональных платформ сокращают доступность эффективных каналов продвижения, усиливают зависимость бизнеса от ограниченного круга цифровых посредников и ограничивают суверенное развитие национальных цифровых экосистем.</p> <p><i>Пункты проблем из полной версии тезисов: 3–4</i></p>	<p>2. Сбалансированная рекламно-платформенная среда</p> <p>Следует формировать постоянные механизмы взаимодействия между государством и рынком при разработке регуляторных мер, а также поддерживать более конкурентную и диверсифицированную рекламно-платформенную среду, снижающую зависимость бизнеса от ограниченного круга глобальных платформ.</p> <p><i>Пункты подходов к решению из полной версии тезисов: 3–4</i></p>
<p>3. Методологическая неопределенность оценки эффективности</p> <p>Отсутствие единых подходов к оценке эффективности медийной рекламы затрудняет отделение собственно рекламного эффекта от алгоритмического отбора, снижает качество управленческих решений и ослабляет роль рекламы как инструмента долгосрочного управления спросом.</p> <p><i>Пункты проблем из полной версии тезисов: 14–16</i></p>	<p>3. Единая система измерения рекламного эффекта</p> <p>Необходимо внедрить единую методологию оценки эффективности медийной рекламы, основанную на сопоставимости тестовых и контрольных групп, сквозной аналитике и регионально адаптированном размещении с учетом неоднородности цифровой среды.</p> <p><i>Пункты подходов к решению из полной версии тезисов: 14–16</i></p>
<p>4. Этические риски рекламы и уязвимость аудитории</p> <p>Цифровая медийная реклама способна усиливать манипулятивное воздействие на уязвимые группы, что требует более четкого разграничения допустимых практик рекламного влияния и пределов ответственности платформ за продвигаемый контент.</p> <p><i>Пункты проблем из полной версии тезисов: 18–21.1</i></p>	<p>4. Этическое регулирование и дифференцированная защита</p> <p>Требуется развитие этического и правового регулирования цифровой рекламы, предусматривающего специальные ограничения для уязвимых аудиторий, повышенные требования к прозрачности рекламных механизмов и дифференцированную ответственность платформ в зависимости от масштаба их влияния на рекламную среду.</p> <p><i>Пункты подходов к решению из полной версии тезисов: 18–21</i></p>
<p>4. ДЕТСТВО ПОД ПАРОЛЕМ: ГДЕ ЗАКАНЧИВАЕТСЯ КОНТРОЛЬ И НАЧИНАЕТСЯ ОТВЕТСТВЕННОСТЬ</p>	
<p>1. Цифровая уязвимость несовершеннолетних</p> <p>Дети и подростки все чаще вовлекаются в опасные интернет-практики и деструктивные сообщества под воздействием цифрового контента, распространяемого через социальные сети и иные онлайн-платформы, что создает риски ранней травматизации, искажения норм социализации и снижения уровня защищенности несовершеннолетних в цифровой среде.</p>	<p>1. Превентивная защита детской цифровой среды</p> <p>Следует развивать механизмы превентивной модерации в детских и подростковых сегментах сети, усиливать мониторинг вредоносных публикаций и продвигать в медиасреде контент, поддерживающий ценность детства, безопасные модели цифровой социализации и недопустимость эксплуатации уязвимости несовершеннолетних.</p>

<p><i>Пункты проблем</i> <i>из полной версии тезисов: 1–1.1</i></p>	<p><i>Пункты подходов к решению</i> <i>из полной версии тезисов: 1–1.1</i></p>
<p>2. Архитектура платформ как источник риска</p> <p>Алгоритмическая логика вовлечения и коммерческие механики платформ часто ориентированы на удержание внимания ребенка, а не на минимизацию рисков для его психического, социального и нравственного благополучия, что усиливает системную уязвимость несовершеннолетних пользователей.</p> <p><i>Пункты проблем</i> <i>из полной версии тезисов: 13–13.1</i></p>	<p>2. Безопасное проектирование цифровой среды для детей</p> <p>Необходима специальная модель ответственности цифровых платформ, предполагающая безопасное проектирование интерфейсов, ограничения на рискованные механики вовлечения, усиленные стандарты модерации и учет возраста пользователя при настройке рекомендаций, контента и цифровых сервисов.</p> <p><i>Пункты подходов к решению</i> <i>из полной версии тезисов: 13–13.5</i></p>
<p>3. Размывание границ ответственности</p> <p>Недостаточная определенность границ между родительским контролем, обязанностями платформ, ролью школы и публичной ответственностью государства создает институциональный разрыв в системе защиты ребенка в цифровой среде.</p> <p><i>Пункты проблем</i> <i>из полной версии тезисов: 6–6.3, 7– 7.1</i></p>	<p>3. Распределенная модель защиты несовершеннолетних</p> <p>Следует закрепить модель распределенной ответственности, при которой родители, образовательные организации, цифровые платформы и государство несут дифференцированные, но взаимосвязанные обязанности по обеспечению цифровой безопасности детей и подростков.</p> <p><i>Пункты подходов к решению</i> <i>из полной версии тезисов: 6–6.3, 7– 7.1</i></p>
<p>4. Дефицит профилактики и цифровой грамотности</p> <p>Недостаток системной профилактики, цифрового просвещения и понятных инструментов помощи детям, родителям и педагогам ослабляет способность общества своевременно выявлять и предупреждать новые риски детской цифровой среды.</p> <p><i>Пункты проблем</i> <i>из полной версии тезисов: 7– 8.2</i></p>	<p>4. Система ранней профилактики и цифрового просвещения</p> <p>Необходима комплексная система цифрового просвещения и ранней профилактики, включающая обучение детей, родителей и педагогов, развитие доступных инструментов жалоб и помощи, а также постоянный мониторинг новых угроз в детской цифровой среде.</p> <p><i>Пункты подходов к решению</i> <i>из полной версии тезисов: 7– 8.4</i></p>

5. БУДУЩЕЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

<p>1. Фрагментация международного регулирования ИИ</p> <p>Отсутствие согласованных международных правил и сохраняющаяся правовая неопределенность в сфере ИИ усиливают регуляторную фрагментацию, затрудняют трансграничный обмен технологиями и снижают предсказуемость глобального технологического взаимодействия.</p> <p><i>Пункты проблем из полной версии тезисов: 1–2</i></p>	<p>1. Многоуровневая система глобального регулирования ИИ</p> <p>Следует формировать многоуровневую модель международного регулирования ИИ, сочетающую базовые правовые рамки, обновляемые технические стандарты, экспертную оценку рисков и механизмы взаимного признания, при одновременном согласовании ИИ-политики с требованиями общественной безопасности.</p> <p><i>Пункты подходов к решению из полной версии тезисов: 1–2</i></p>
<p>2. Борьба за институциональное лидерство в ИИ</p> <p>Будущее ИИ определяется не только технологическими возможностями, но и борьбой за право задавать стандарты, допустимые пределы и архитектуру глобального управления, что создает риск концентрации нормативной власти у ограниченного круга государств и корпораций.</p> <p><i>Пункты проблем из полной версии тезисов: 3</i></p>	<p>2. Инклюзивное глобальное управление ИИ</p> <p>Необходимо обеспечить более инклюзивную модель глобального управления ИИ, в которой выработка стандартов и процедур не монополизирована технологическими лидерами, а учитывает интересы государств с различным уровнем технологического развития и различными правовыми традициями.</p> <p><i>Пункты подходов к решению из полной версии тезисов: 3–3.3</i></p>
<p>3. Культурная и языковая асимметрия ИИ</p> <p>Универсализация ИИ-моделей без учета языкового, культурного и мировоззренческого разнообразия создает риск систематического искажения знаний, снижения качества сервисов для недоминирующих языков и навязывания ограниченного набора когнитивных и нормативных установок.</p> <p><i>Пункты проблем из полной версии тезисов: 29.2–29.7</i></p>	<p>3. Мультикультурная и мультиязычная архитектура ИИ</p> <p>Следует выработать механизмы культурно и лингвистически чувствительной настройки ИИ, включая поддержку малых языков, стандарты представления чувствительного контента, оценку качества сервисов с учетом контекста пользователя и независимую экспертизу эталонных ответов по социально значимым вопросам.</p> <p><i>Пункты подходов к решению из полной версии тезисов: 29.2–29.7</i></p>
<p>4. Несоразмерность внедрения и общественных гарантий</p> <p>Без четких критериев допустимости применения ИИ в социально значимых сферах масштабы его внедрения начинают определяться логикой технологической экспансии, а не балансом прав, безопасности и общественного интереса.</p> <p><i>Пункты проблем из полной версии тезисов: 2</i></p>	<p>4. Приоритет общественной безопасности и правовых пределов</p> <p>Необходимо закрепить принцип, согласно которому внедрение ИИ должно определяться не только технологической готовностью, но и прохождением процедур правовой, этической и социальной оценки, подтверждающих совместимость конкретных решений с общественной безопасностью и фундаментальными правами.</p> <p><i>Пункты подходов к решению из полной версии тезисов: 2–2.3</i></p>

6. КТО ОПРЕДЕЛЯЕТ ПОГОДУ: ОБЛАЧНЫЕ СЕРВИСЫ В ЭПОХУ СУВЕРЕНИТЕТА

<p>1. Стратегическая зависимость от транснациональной облачной инфраструктуры</p> <p>Зависимость государств и бизнеса от транснациональных облачных инфраструктур усиливает их политическую, экономическую и технологическую уязвимость, поскольку контроль над хранением, обработкой и управлением данными концентрируется у внешних поставщиков цифровых ресурсов.</p> <p><i>Пункты проблем из полной версии тезисов: 1–1.1</i></p>	<p>1. Устойчивый и недискриминационный доступ к облачным ресурсам</p> <p>Требуется формирование режима устойчивого и недискриминационного доступа к облачным ресурсам, сочетающего правовые гарантии доступа, механизмы резервирования инфраструктуры, требования к прозрачности обработки данных и меры по снижению зависимости от отдельных провайдеров.</p> <p><i>Пункты подходов к решению из полной версии тезисов: 1–1.1</i></p>
<p>2. Экстерриториальная юрисдикция и утрата контроля над данными</p> <p>Подчинение облачных провайдеров праву государств их регистрации создает условия для экстерриториального доступа к данным, правовой неопределенности и ослабления цифрового суверенитета пользователей и государств.</p> <p><i>Пункты проблем из полной версии тезисов: 2–2.2</i></p>	<p>2. Суверенное и ответственное управление данными</p> <p>Необходимо выработать международные и национальные механизмы суверенного управления данными, включая разграничение юрисдикции, специальные гарантии от экстерриториального вмешательства и правила обращения с критически значимой информацией в трансграничной облачной среде.</p> <p><i>Пункты подходов к решению из полной версии тезисов: 2–2.4</i></p>
<p>3. Технологическая замкнутость и инфраструктурная концентрация</p> <p>Ограниченная переносимость данных между облаками и концентрация инфраструктуры у небольшого числа провайдеров снижают конкуренцию, закрепляют зависимость пользователей и ограничивают их технологическую мобильность.</p> <p><i>Пункты проблем из полной версии тезисов: 6–7.1</i></p>	<p>3. Интероперабельность и диверсификация облачной среды</p> <p>Следует внедрять единые стандарты переноса данных и интероперабельности, развивать национальные и региональные облачные экосистемы, обеспечивать совместимость платформ и формировать распределенную инфраструктурную модель, снижающую зависимость от ограниченного круга внешних поставщиков.</p> <p><i>Пункты подходов к решению из полной версии тезисов: 6–7.2</i></p>
<p>4. Облачный суверенитет как вопрос стратегической автономии</p> <p>Облачный рынок становится пространством столкновения суверенитета, конкуренции и технологической зависимости, в котором государства и пользователи ограничены в возможности полноценно контролировать критическую инфраструктуру, условия доступа к цифровым ресурсам и устойчивость своих сервисов.</p> <p><i>Пункты проблем из полной версии тезисов: весь раздел, прежде всего 1–7.1</i></p>	<p>4. Стратегия облачного суверенитета</p> <p>Стратегически необходима модель облачного суверенитета, основанная на диверсификации провайдеров, интероперабельности, резервировании критических мощностей, поддержке национальных инфраструктурных решений и международных правилах, исключающих дискриминационный доступ к облачным сервисам.</p> <p><i>Пункты подходов к решению из полной версии тезисов: 1–7.2</i></p>