Космический интернет	
Проблема	Способ/подход к решению
<p>1. Геополитическая и технологическая зависимость в сфере спутниковых коммуникаций</p> <p>Преобладание западных (особенно американских) спутниковых систем, таких как Starlink, ставит под угрозу суверенитет и безопасность отдельных государств, ограничивает развитие национальных технологий и вынуждает к стратегическому выбору между созданием собственных решений и зависимостью от внешних.</p> <p><i>Пункты проблем из полной версии тезисов:</i> 1.1, 4.1, 6.1</p>	<p>1. Развитие национального потенциала в космической сфере: от технологий до кадровой базы</p> <p>Создание конкурентоспособной отечественной спутниковой системы через инвестиции в инфраструктуру, образование, кадры и стимулирование частных инициатив.</p> <p><i>Пункты подходов из полной версии тезисов:</i> 1.1 - 1.7, 6.1</p>
<p>2. Регуляторные и организационные вызовы в условиях глобализации космического пространства</p> <p>Отсутствие международной координации, единых правовых механизмов и эффективного контроля в условиях трансграничного характера спутникового Интернета и космических данных усложняет развитие и эксплуатацию спутниковых систем.</p> <p><i>Пункты проблем из полной версии тезисов:</i> 3.1, 4.1, 5.1</p>	<p>2. Формирование международно согласованной правовой и институциональной среды</p> <p>Создание единых правил игры на орбите и в информационном пространстве через международные платформы, соглашения, и системную координацию усилий между странами.</p> <p><i>Пункты подходов из полной версии тезисов:</i> 2.2, 2.3, 3.1 - 3.3, 4.1, 4.2, 5.1, 5.2, 7.2</p>
<p>3. Экологические и научные вызовы и риски ускоренного развития спутниковых технологий</p> <p>Массовые запуски спутников порождают экологические проблемы (углеродный след, загрязнение орбиты) и влияют на научные исследования, в том числе создавая помехи астрономам. Одновременно наблюдается нехватка орбитальных слотов и ресурсов для поддержания устойчивости существующей инфраструктуры.</p> <p><i>Пункты проблем из полной версии тезисов:</i> 2.1, 7.1, 8.1</p>	<p>3. Устойчивое развитие: баланс между технологическим прогрессом, наукой и экологией</p> <p>Минимизация негативного воздействия космической деятельности на экологию и научные исследования через новые технологии и международные договорённости.</p> <p><i>Пункты подходов из полной версии тезисов:</i> 2.1, 7.1, 7.2, 8.1 - 8.3</p>

Кибербезопасность	
Проблема	Способ/подход к решению
<p>1. Угрозы персональной и корпоративной безопасности данных в условиях цифровизации</p> <p>Массовое распространение цифровых сервисов усиливает риски утечки и неправомерного использования персональных и корпоративных данных, что требует комплексной и технологически актуальной системы защиты, ориентированной не только на соответствие формальным требованиям, но и на реальные угрозы.</p> <p><i>Пункты проблем из полной версии тезисов:</i> 1.1 - 1.3, 6.1, 6.2, 9.1, 12.1, 13.1</p> <p>2. Структурные и организационные дефициты в области информационной безопасности</p> <p>Системная слабость корпоративного и государственного управления ИБ проявляется в разрыве между требованиями регуляторов, реальными угрозами и целями бизнеса. Также остро стоит проблема координации между подразделениями, нехватка общих стандартов и институциональных рамок.</p> <p><i>Пункты проблем из полной версии тезисов:</i> 3.1, 4.1, 5.1, 7.1, 8.1, 10.1, 11.1, 13.1</p> <p>3. Цифровое неравенство и социальные риски в киберпространстве</p> <p>Резкая цифровизация обострила проблему неравного доступа к технологиям, особенно среди уязвимых групп населения. Недостаток навыков, оборудования и осведомлённости делает таких пользователей лёгкой целью для мошенников и усиливает социальные риски.</p> <p><i>Пункты проблем из полной версии тезисов:</i> 2.1, 9.1</p>	<p>1. Развитие технологий и инфраструктуры кибербезопасности</p> <p>Адаптация и внедрение передовых технологий (ИИ, блокчейн, цифровые двойники и т.д.), создание стандартов и инфраструктуры для обеспечения устойчивой цифровой среды, особенно в чувствительных областях (персональные данные, ИИ, цепочки поставок).</p> <p><i>Пункты подходов из полной версии тезисов:</i> 1.2, 1.3, 6.1, 6.3, 6.4, 7.1, 7.2, 8.1, 10.1, 11.1</p> <p>2. Подготовка кадров и развитие культуры кибербезопасности</p> <p>Формирование системы образования и непрерывного повышения квалификации в области ИБ, развития у сотрудников навыков критического мышления, понимания бизнес-процессов и ответственности. Внедрение ИБ как ценности, а не формального требования.</p> <p><i>Пункты подходов из полной версии тезисов:</i> 1.4, 3.1 - 3.3, 4.1, 5.1 - 5.4, 6.2, 9.1</p> <p>3. Интеграция ИБ в бизнес и межотраслевое взаимодействие</p> <p>Интеграция ИБ в стратегию бизнеса и операционные процессы, преодоление разрыва между безопасностью и управлением. Развитие механизмов взаимодействия между компаниями, регуляторами и отраслями.</p> <p><i>Пункты подходов из полной версии тезисов:</i> 3.2, 3.3, 4.1, 4.2, 12.1, 13.1</p> <p>4. Цифровая инклюзия и доступность технологий</p> <p>Создание доступной и безопасной цифровой среды для всех категорий граждан, особенно уязвимых групп, включая пожилых. Повышение цифровой грамотности и доступ к современным устройствам.</p> <p><i>Пункты подходов из полной версии тезисов:</i> 2.1, 8.2</p>

Открытый код	
Проблема	Способ/подход к решению
<p>1. Отсутствие устойчивой экосистемы и поддержки для разработчиков открытого ПО</p> <p>Открытое ПО развивается усилиями сообщества, но при этом страдает от недостаточной монетизации, отсутствия стабильной технической поддержки и слабой институциональной поддержки со стороны государства или бизнеса, что ограничивает потенциал роста и внедрения Open Source-решений, особенно в критически важных и импортозамещающих сферах.</p> <p><i>Пункты проблем из полной версии тезисов:</i> 1.1, 3.1, 5.1, 7.1, 8.1</p> <p>2. Правовая и нормативная неопределенность в сфере Open Source</p> <p>Открытое ПО активно используется, но его лицензии и правовая природа плохо согласуются с локальным законодательством, особенно в странах СНГ, что создает юридические риски, препятствует интеграции в бизнес-процессы и тормозит развитие правовой базы для поддержки Open Source в национальных цифровых стратегиях.</p> <p><i>Пункты проблем из полной версии тезисов:</i> 1.1, 2.1, 3.1, 4.1, 9.1</p> <p>3. Повышенные риски безопасности и устойчивости при использовании открытого ПО</p> <p>Прозрачность кода в Open Source одновременно является его преимуществом и уязвимостью. Недостаток контроля над изменениями, слабая защищённость репозиторий, возможность использования уязвимостей и отсутствие централизованной ответственности - всё это делает такие решения потенциально опасными для критических инфраструктур и корпоративных систем.</p> <p><i>Пункты проблем из полной версии тезисов:</i> 2.1, 5.2, 6.1, 7.1, 8.1</p>	<p>1. Развитие устойчивой Open Source-экосистемы</p> <p>Создание условий для устойчивого развития открытого ПО: поддержка разработчиков, стимулирование монетизации, развитие локальной инфраструктуры и импортозамещения</p> <p><i>Пункты подходов из полной версии тезисов:</i> 1.1, 3.2, 3.3, 6.1</p> <p>2. Правовая адаптация и стандартизация лицензирования</p> <p>Адаптация и локализация лицензионных норм Open Source под национальные реалии с целью устранения правовой неопределенности, гармонизации интересов разработчиков и бизнеса.</p> <p><i>Пункты подходов из полной версии тезисов:</i> 4.1, 9.1, 9.2</p> <p>3. Повышение безопасности и управляемости Open Source-решений</p> <p>Устранение технических и организационных рисков при использовании открытого кода за счёт усиления контроля, сертификации, безопасности и защиты критической инфраструктуры.</p> <p><i>Пункты подходов из полной версии тезисов:</i> 2.1, 5.3, 6.1</p>

Глобальный диалог и цифровая повестка

Проблема	Способ/подход к решению
<p>1. Проблема регулирования и мониторинга цифрового контента и пользователей</p> <p>Совокупность проблем, связанных с отсутствием четких механизмов контроля и мониторинга за действиями пользователей в цифровом пространстве, а также отсутствием консенсуса по узконаправленным вопросам.</p> <p><i>Пункты проблем из полной версии тезисов: 1.1, 2.1</i></p> <p>2. Проблемы цифрового суверенитета и саморегулирования глобальных цифровых платформ</p> <p>Проблемы, касающиеся баланса между контролем за цифровым пространством на уровне государств и саморегулированием глобальных цифровых платформ.</p> <p><i>Пункты проблем из полной версии тезисов: 4.1, 4.2, 5.1.</i></p> <p>3. Проблемы управления и регулирования технологий искусственного интеллекта (ИИ)</p> <p>Вызовы, связанные с быстрым развитием и управлением технологиями ИИ, которые ставят перед человечеством новые этические, правовые и технические задачи.</p> <p><i>Пункты проблем из полной версии тезисов: 3.1</i></p>	<p>1. Структурирование процессов обсуждения и мониторинга</p> <p>Разработка и внедрение структурированных процессов, направленных на эффективное обсуждение узких и общих вопросов для достижения консенсуса, а также создание механизмов контроля за пользователями и контентом в цифровом пространстве.</p> <p><i>Пункты подходов из полной версии тезисов: 1.1, 2.1</i></p> <p>2. Ответственное управление ИИ и цифровыми платформами</p> <p>Внедрение системы сертификации и контроля для ИИ-систем и цифровых платформ, обеспечивающее безопасность, этичность и прозрачность технологий, с учетом локальных и международных стандартов.</p> <p><i>Пункты подходов из полной версии тезисов: 3.1, 3.2, 4.1, 4.2, 4.5</i></p> <p>3. Регулирование технологий ИИ с этической и правовой основой</p> <p>Разработка механизмов управления ИИ, включая сертификацию, установление общих принципов и создание гибкой системы регулирования, стимулируя инновации и соблюдая этические нормы.</p> <p><i>Пункты подходов из полной версии тезисов: 3.1, 3.2</i></p>

Цифровая деструктивность	
Проблема	Способ/подход к решению
<p>1. Проблемы психоэмоционального состояния пользователей в цифровом пространстве</p> <p>Проблемы, связанные с влиянием технологий на психоэмоциональное состояние пользователей, включая когнитивную перегрузку, зависимость от социальных сетей, а также возникновение психических расстройств и стрессов от чрезмерного пребывания в интернете.</p> <p><i>Пункты проблем из полной версии тезисов:</i> 1.1, 3.1, 4.1, 4.2</p>	<p>1. Создание программ повышения осознанности и продуктивности пользователей в цифровом пространстве</p> <p>Подход ориентирован на улучшение психоэмоционального состояния пользователей через обучение продуктивности, цифровой гигиене и умению разгружать информационные потоки.</p> <p><i>Пункты подходов из полной версии тезисов:</i> 1.1, 1.2, 4.4</p>
<p>2. Проблемы цифровой зависимости и воздействия технологий на поведение</p> <p>Проблемы, связанные с цифровой зависимостью, включая чрезмерное времяпрепровождение в интернете, зависимость от технологий, а также сложность организации цифровой детоксикации.</p> <p><i>Пункты проблем из полной версии тезисов:</i> 2.1, 3.2</p>	<p>2. Развитие альтернативных способов общения и формирование сбалансированного подхода между онлайн и офлайн активностями</p> <p>Подход предполагает стремление к уменьшению влияния цифровых технологий и увеличение внимания к реальным социальным связям, а также развитие физической и культурной активности.</p> <p><i>Пункты подходов из полной версии тезисов:</i> 2.1, 3.3, 4.1, 4.3</p>
<p>3. Проблемы этики и безопасности в цифровом пространстве</p> <p>Проблемы, связанные с этическими нормами и безопасностью в интернете, включая отсутствие четких норм поведения и уязвимость пользователей к мошенничеству.</p> <p><i>Пункты проблем из полной версии тезисов:</i> 5.1, 6.1</p>	<p>3. Разработка этических норм и регулирование поведения пользователей в цифровом пространстве</p> <p>Направлен на создание этичного и безопасного цифрового пространства через разработку норм поведения и внедрение мягкого регулирования.</p> <p><i>Пункты подходов из полной версии тезисов:</i> 6.1 - 6.4</p>

Цифровая дезинформация и медиаэффекты

Проблема	Способ/подход к решению
<p>1. Низкое качество и недостоверность информации в цифровом пространстве</p> <p>Проблемы, связанные с распространением и проверкой информации в Интернете, включая манипуляции с контентом, использование дипфейков и феномен постправды, которые влияют на восприятие реальности и доверие к источникам.</p> <p><i>Пункты проблем из полной версии тезисов:</i> 1.1 - 1.3, 2.1, 5.1</p> <p>2. Снижение доверия к цифровым медиа и информационным источникам</p> <p>Вопросы доверия и усталости от проверки фактов, сжигание доверия к СМИ и источникам информации в целом, а также общая недоверчивость к цифровым источникам в связи с их неоднозначностью и фрагментацией.</p> <p><i>Пункты проблем из полной версии тезисов:</i> 4.1, 4.2</p> <p>3. Фрагментация медиапространства и ухудшение коммуникации в обществе</p> <p>Проблемы, связанные с фрагментацией медиапространства, из-за которой теряется общая тема для обсуждения и снижается уровень коммуникации в обществе.</p> <p><i>Пункты проблем из полной версии тезисов:</i> 3.1</p>	<p>1. Повышение качества и достоверности информации</p> <p>Создание эффективных механизмов для проверки информации, повышение осведомленности пользователей и снижение дезинформации в цифровом пространстве через использование технологий и установление этических стандартов.</p> <p><i>Пункты подходов из полной версии тезисов:</i> 1.1 - 1.3, 2.1, 2.2, 4.1 - 4.3, 4.5, 4.7, 5.1, 5.3, 5.4</p> <p>2. Развитие критического мышления и медиаграмотности</p> <p>Подход фокусируется на образовательных инициативах, направленных на развитие у пользователей критического мышления, медиаграмотности и навыков осознанного восприятия контента, что поможет в борьбе с дезинформацией и повысит уровень доверия к источникам.</p> <p><i>Пункты подходов из полной версии тезисов:</i> 1.2, 1.4, 3.2, 3.3, 4.5</p> <p>3. Укрепление институциональной верификации и прозрачности информации</p> <p>Подход направлен на повышение доверия к информации через внедрение независимой верификации контента, создание институциональных механизмов для подтверждения достоверности данных и их источников.</p> <p><i>Пункты подходов из полной версии тезисов:</i> 4.1, 4.2, 4.3, 4.7, 5.4</p>