

Космический интернет	
Проблема	Способ/подход к решению
1.1. Проблема технологической зависимости: доминирование американских спутниковых систем, таких как Starlink, и отсутствие у России эффективных низкоорбитальных спутников создают угрозу национальной безопасности и препятствуют развитию отечественных технологий связи	1.1. Развитие и финансирование национальных государственных проектов низкоорбитальных спутников, в том числе поддержка государственных и частных проектов, например Сфера или Бюро 1440 1.2. Разработка мер привлечения компетентных специалистов (гранты, система поощрений, освобождение от налогообложения, локации с развитой инфраструктурой не только научной направленности, но и направленной на свободную социализацию и коммуникацию специалистов), обеспечение необходимых лабораторий/центров, оснащенных современным оборудованием 1.3. Увеличение финансирования образовательных программ в области космических технологий, спутниковой связи и смежных дисциплин. Это поможет подготовить новое поколение специалистов. 1.4. Развитие взаимодействия с дружественными странами для совместной разработки и запуска спутников, что позволит разделить затраты и ускорить внедрение технологий. 1.5. Выработка политико-правовых условий, в том числе путем создания экспериментальных правовых режимов в целях содействия внедрению собственных технологических решений 1.6. Упростить получение налоговых льгот, грантов и субсидий для организаций, занимающихся предоставлением доступа к Интернету с использованием низкоорбитальных спутников. 1.7. Потенциальное внедрение национальных спутниковых систем на основе сетей 5G и 6G. За счет таких отечественных систем в будущем возможно повышение связности территорий страны.
2.1. Проблема глобальной нехватки орбитального пространства для спутников, при одновременном недостатке возможностей для обновления геостационарных спутников.	2.1. Создание дорожной карты обновления геостационарных спутников с возможностью привлечения средств частных компаний на их обновление и модернизацию. 2.2. Создание на базе МСЭ единой платформы для организаций, специализирующихся на запуске спутников и управлении орбитальными системами, с целью выработки единой и географически справедливой политики в области управления орбитальным пространством. 2.3. Разработка концепции «орбитальных парков» - зон, где спутники могут располагаться на определённых орбитах с учетом минимизации взаимодействия и риска столкновений.
3.1. Проблема регулирования и усложнение контроля над потоками спутниковых данных в условиях трансграничного характера информационного пространства.	3.1. Выработка единого международного механизма по контролю и систематизации спутниковых данных.

	3.2 Разработка новых решений, в том числе с использованием ИНС, в части безопасности и управления потоками данных, передаваемых через спутниковые системы связи - внедрение решений для фильтрации трафика позволит ограничивать доступ к подозрительному или потенциально опасному содержанию, доработка инструментов учета и анализа трафика может обеспечить прозрачность и предотвратить нецелевой доступ, адаптируясь к особенностям информационной среды спутниковой связи. 3.3. Предусмотреть механизм внедрения решений для мониторинга трафика на аппаратном или программном уровне для отечественных производителей терминалов спутниковой связи. Для иностранных провайдеров рассмотреть вариант установления условий, включающих локализацию данных, размещение серверов мониторинга и интеграцию наземных станций с системами контроля. При несоблюдении требований предусмотреть ограничение работы терминалов вблизи границ и ключевых объектов или применение мер по подавлению сигналов.
4.1. Отсутствие унифицированного нормативно-правового международного подхода по отношению к передаче данных через спутниковый Интернет.	4.1. Ввести международный нормативно-правовой подход к передаче данных через спутниковый Интернет, дополнив существующий механизм Договора о космосе 1967 г. учетом "конечной точки" - государства или субъекта, получающего данные, наряду с государством запуска, для обеспечения более полного и гибкого регулирования ответственности за использование данных, передаваемых посредством спутниковых систем. 4.2. Разработка документа, определяющего вопросы взаимодействия компаний и государств, распределения ответственности в части потоков данных. Данные принципы первоначально могут быть закреплены в виде меморандума о сотрудничестве, позже устоявшийся порядок взаимодействия может быть закреплён международными договорами и в национальных законодательствах.
5.1. Низкая координация исследований Луны	5.1. Поддержка деятельности и развитие международных дискуссионных площадок организованных, например, на базе ООН по вопросам космического пространства (UNOOSA), или в рамках Повестки «Космос-2030»: космос как двигатель устойчивого развития для выработки единой международной политики в области исследования Луны <i>В н.в. усилия фрагментированы, глобального консенсуса нет. Тезис подчеркивает необходимость усиления этих платформ, что пока остается вызовом. Решения на площадках ООН зачастую носят рекомендательный характер из-за чего усилия крупнейших игроков фрагментированы</i> 5.2. Требуется объединение усилий и оптимизация совместной работы - развитие инфраструктуры для передачи данных и синхронизации миссий в реальном времени через орбитальные узлы связи создаст основу для эффективного взаимодействия.

	Также стоит рассмотреть создание общей системы планирования, такой как единый график лунных исследований, чтобы ученые и специалисты могли вместе формировать будущее освоения Луны. <i>Частичные механизмы есть (инфраструктура связи, международные соглашения), но такие усилия носят разрозненный характер и не объединены в глобальную систему. Тезис предлагает более интегрированный подход, которого сегодня не хватает, особенно в части единого графика и синхронизации через орбитальные узлы для всех участников.</i>
6.1. Проблема поиска оптимальной стратегии создания спутниковой системы связи в условиях имеющегося выбора между безопасностью спутниковых данных и нерентабельностью создания собственной спутниковой системы.	6.1. Создание экспертной комиссии (включающей государственный, частный, научный сектор) для определения приоритетных направлений использования спутниковой связи там, где она незаменима. <i>Например, в Арктике, транспортных коридорах, критической инфраструктуре (нефтегаз, энергетика, военные объекты), а также использование в качестве резервных каналов связи</i>
7.1. Конфликт между технологическим развитием и исследованиями космоса для астрономов - запуск спутников связи на низкой орбите создает «помехи» при исследовании объектов.	7.1. Создать новые механизмы подавления нежелательных помех для проведения корректных исследовательских проектов. 7.2 Создание международных платформ для диалога между технологическими компаниями и научным сообществом поможет учитывать потребности астрономов при планировании орбитальных миссий. Также стоит развивать совместные инициативы, такие как согласование зон размещения спутников, чтобы минимизировать их влияние на наблюдения космоса.
8.1. Прогрессирование экологических проблем: запуски спутников могут иметь негативное воздействие на окружающую среду, включая выбросы углерода и другие загрязнения.	8.1. Оптимизация процессов запуска для уменьшения количества необходимых запусков (использование многоразовых ракет, которые могут быть восстановлены и использованы повторно) 8.2. Разработка технологий удаления космического мусора, чтобы предотвратить загрязнение орбиты. 8.3. Направить усилия на усовершенствование существующих механизмов, таких как экологические стандарты Международной организации гражданской авиации и национальные регуляции, путем признания юридических лиц, лицами, эксплуатирующими объекты негативного воздействия на окружающую среду, подлежащие региональному государственному экологическому надзору. <i>Эти платежи, рассчитываемые на основе объема выбросов углерода и других загрязнений при запусках, будут направляться на финансирование проектов по восстановлению окружающей среды и разработку более чистых технологий космических пусков, дополняя текущие усилия по снижению углеродного следа в отрасли.</i>

Кибербезопасность	
Проблема	Способ/подход к решению
1.1. Обеспечение безопасности и конфиденциальности персональных финансовых данных, включая банковские вклады, а также разработка комплексных мер по противодействию мошенничеству в цифровой экономике. 1.2. Формирование безопасного информационно-технического пространства в сфере защиты конфиденциальной информации и персональных данных. 1.3. Проблема создания эффективных механизмов защиты персональных данных граждан.	1.1. Совершенствование мер ответственности для сотрудников, работающих с конфиденциальными данными, с акцентом на профилактику нарушений и повышение профессиональных стандартов в финансовой и смежных сферах. 1.2. Расширение применения систем искусственного интеллекта и машинного обучения, уже используемых для мониторинга подозрительных действий, с целью повышения эффективности выявления мошенничества и защиты данных в цифровой экономике. 1.3. Использование технологий распределённых реестров для безопасного хранения данных, обеспечивающих их защиту от компрометации и несанкционированного доступа, с учетом текущих и будущих вычислительных возможностей. 1.4. Усиленная подготовка специалистов в сфере ИБ через прохождение современных курсов повышения квалификации, в том числе государственных программ
2.1. Проблема цифрового неравенства, в особенности среди пожилого населения РФ: пандемия ускорила цифровизацию госсектора, но пожилые люди сталкиваются с трудностями из-за недостатка техники, материальных ресурсов и навыков работы с технологиями, что повышает их уязвимость перед мошенниками.	2.1. Повышение цифровой грамотности и технологической доступности: – Организация доступных «кружков» для пожилых, в т.ч. по освоению технических навыков и медийной грамотности (во всех регионах страны). – Введение государственных финансовых мер поддержки, таких как субсидии на покупку современных устройств (например, раз в 5 лет частичное покрытие стоимости устройств).
3.1. Проблема несоответствия целей информационной безопасности целям бизнеса в рамках существующих бизнес-моделей и приоритетов.	3.1. Обеспечение открытости ИБ и бизнеса посредством тесного взаимодействия на стратегических сессиях, проведение обучения сотрудников по рискам ИБ на примере конкретных инцидентов и уязвимостях, последствий их апробации. 3.2. Гармонизация приоритетов ИБ и бизнеса: разработка программ обучения для специалистов ИБ, направленных на понимание бизнес-процессов, потребностей руководства и эффективного представления услуг ИБ, чтобы сделать безопасность неотъемлемой частью бизнес-стратегии. 3.3. Создание программ обучения для специалистов по информационной безопасности, направленных на углублённое понимание бизнес-процессов, стратегических целей компании и методов адаптации ИБ-подходов под эти задачи.

4.1. Проблема обеспечения эффективного взаимодействия между отделом информационной безопасности и другими подразделениями компании.	4.1. Содействие совместной разработки сотрудниками ИБ и сотрудниками отделов, осуществляющих конкретные операции, бизнес-процессов в формате кросс-функциональных команд с оценкой момента выявления уязвимости и инцидента и порядка их предупреждения /выявления и устранения. <i>В том числе, возможно расширение подобных инициатив в направлении создания программ обучения по интеграции работников ИБ в существующие бизнес-процессы с учётом целей и потребностей организаций.</i> 4.2 Усиление интеграции ИБ в бизнес-процессы, в том числе за счет выделения достаточных финансовых и человеческих ресурсов на ИБ, регулярное повышение квалификации сотрудников ИБ, а также внедрение контроля со стороны высшего руководства для обеспечения соблюдения инструкций и координации действий между отделами.
5.1. Проблема фокуса специалистов ИБ на соблюдении требований регуляторов вместо противодействия реальным угрозам. <i>Недостаточное понимание специалистами ИБ и компанией целей и целесообразности выстраиваемых процессов защиты (не только соответствие требованиям регулятора, но и противодействие реальным угрозам).</i>	5.1. Повышение осведомленности и качества кадров в ИБ, в том числе за счет внедрения тренингов, фокусирующихся на анализе конкретных угроз и выстраивании процессов защиты, а также развитие культуры осознанного подхода к ИБ, где цели безопасности связаны с реальными рисками. <i>Данная проблема не техническая. Соответственно решение должно быть в ключе "человек-человек". Скорее всего, также, стоит разработать единое руководство для компаний и специалистов, потому что проблема целесообразности применима в глобальном смысле.</i> 5.2. Формирование компетентного кадрового состава, в целях создания системы подбора, обучения и развития специалистов ИБ, направленной на выявление кандидатов с высокими навыками критического мышления, пониманием целей процессов защиты и способности принимать решения, соответствующих стратегическим задачам организации. 5.3. Запуск пилотных проектов по модернизации системы образования всех уровней для подготовки специалистов ИБ (в отдельных регионах или учреждениях для оценки эффекта и дальнейшего масштабирования). <i>Например, ввести ИБ как факультатив в школах или обязательный курс в технических вузах.</i> 5.4. Развитие государственной поддержки подготовки кадров в ИБ, за счет выделения субсидий на повышение квалификации преподавателей вузов и колледжей по новым программам для IT-специальностей с акцентом на ИБ, а также за счет оптимизации и интеграция существующих программ в сфере кибербезопасности для подготовки специалистов, востребованных как в госсекторе, так и в бизнесе.
6.1. Обеспечение безопасности данных в сфере искусственного интеллекта (защита от DoS-атак, данных пользователей и т.д.) 6.2. Существующие механизмы защиты данных в РФ недостаточно адаптированы к специфике ИИ-систем.	6.1. Направление усилий на разработку механизмов эффективного перехода к локализации критически важных ИИ-систем <i>В соответствии с текущим трендом по локализации данных (ФЗ-242) требуется преодоление сопротивления бизнеса из-за роста затрат и сложностей такого</i>

<i>Отсутствие единых стандартов безопасности, требований к хранению и обработке персональных данных и конфиденциальной информации, слабая интеграция современных методов защиты.</i>	<i>перехода, в частности требуются механизмы содействия по установке ПО, баз данных и ИИ-систем на собственных вычислительных ресурсах организаций, а также по ограничению использования облачных сервисов процессами, не связанными с чувствительными данными, с обязательным аудитом их безопасности.</i> 6.2. Разработка программ и проведение тренингов по кибербезопасности для сотрудников, работающих с ИИ-системами. 6.3. Создание экспертной комиссии по регулированию систем искусственного интеллекта и разработке мер безопасной разработки и эксплуатации систем искусственного интеллекта. 6.4 Разработка отраслевых стандартов. Создание специальных нормативных актов для ИИ систем. Среди требований должны быть анонимизация данных, логирование доступа к данным в ИИ моделях и сертификация алгоритмов на соответствие стандартам безопасности.
7.1. Уязвимость цепочек поставок и ключевых компаний к кибератакам на слабые звенья угрожает экономике и безопасности России из-за недостатка единых стандартов защиты и координации.	7.1. Проведение совместных подконтрольных киберучений в отношении сотрудников, информационных систем партнеров 7.2 Создание цифровых двойников цепочек поставок. Моделирование кибератак на виртуальных копиях цепочек, автоматическое выявление слабых звеньев.
8.1. Юридическая неоднозначность и коллизии в нормативно-правовых актах, регулирующих сбор, обработку и хранение персональных данных, создают правовую неопределенность для бизнеса и государства, затрудняют обеспечение безопасности данных и повышают риски.	8.1. Закрепить в нормативных актах, регулирующих персональные данные, понятные и однозначные определения ключевых понятий на основе анализа практики и предложений бизнеса, чтобы устранить юридические противоречия. 8.2. Проведение информационной кампании - разработать и распространить через отраслевые платформы, СМИ и курсы повышения квалификации доступные материалы (инфографику, памятки и видео) с разъяснением терминов, связанных с персональными данными, и последствий их неверного применения.
9.1. Растущая уязвимость сотрудников организаций к методам социальной инженерии, включая целевые фрод-атаки с использованием искусственного интеллекта, угрожает безопасности данных и устойчивости бизнеса, усиливая риски в условиях недостаточной подготовки персонала и отсутствия единых защитных мер.	9.1 Разработка оптимальной системы безопасности против применения методов социальной инженерии по отношению к сотрудникам организации через повышение безопасности данных в организации (введение различных уровней доступа сотрудников к данным организации, систематическая смена паролей), а также обучение сотрудников (тренинги, повышение квалификации).
10.1 Широкая дифференциация уязвимостей информационной инфраструктуры.	10.1 Внедрение и поддержка комплексного подхода к повышению киберустойчивости бизнеса через развитие национальных стандартов мониторинга операций и регулярных тестов на уязвимости (пентестов) критичных активов, с учетом интересов клиентов и текущих нормативных требований.
11.1 Недостаточная ясность требований законодательства и отсутствие единых рекомендаций от госорганов затрудняют правоприменение и создают риски неоднозначной интерпретации норм, что снижает эффективность внедрения технологий и защиты данных.	11.1 Обеспечить бизнесу понятность и предсказуемость законодательства в сфере ИИ и кибербезопасности через разработку единых практических рекомендаций и разъяснений от госорганов, дополненных прозрачными пояснениями к новым нормам права.

	<i>Например, внедрить практику подготовки детальных пояснительных записок к законопроектам с примерами применения норм, привлекая судебное и экспертное сообщество для формирования единообразных подходов. Организовать регулярный сбор обратной связи от бизнеса через отраслевые площадки для актуализации рекомендаций и устранения противоречий.</i>
12.1 Кибератаки на ключевые производственные ресурсы (материальные, интеллектуальные, людские и финансовые) создают угрозу устойчивости бизнеса и экономики, усиливая уязвимости в условиях недостаточной защищенности и координации мер противодействия.	12.1. Необходимость учета отраслевых особенностей и ускорения межведомственного взаимодействия. <i>Например, через интеграцию существующих инструментов: усилить стандарты кибербезопасности с акцентом на обучение персонала и защиту данных, адаптировав их под специфику отраслей, а также внедрить мониторинг угроз и анализ инцидентов на базе существующих систем, дополнив их рекомендациями для бизнеса по минимизации рисков; организовать обмен информацией об атаках через отраслевые ассоциации и платформы госуслуг для оперативного реагирования.</i>
13.1. Нежелание компаний открыто раскрывать данные об уязвимостях и кибератаках из-за репутационных рисков ограничивает обмен опытом, разработку отраслевых стандартов и совместное противодействие угрозам в условиях недостаточной прозрачности и доверия.	13.1. Стимулировать открытость через адаптацию текущих мер: внедрить анонимизированный обмен данными об инцидентах через платформы, организовать отраслевые площадки при поддержке ассоциаций и госуслуг для обмена лучшими практиками без ущерба репутации, а также рассмотрение возможности поощрения-вознаграждения за найденные уязвимости (в том числе механизм bug bounty).

Открытый код	
Проблема	Способ/подход к решению
1.1 Разработчики, использующие открытый код, сталкиваются с трудностями монетизации своих решений, что ограничивает развитие экосистемы открытого ПО и инноваций в условиях недостаточной поддержки и регулирования этого процесса.	1.1 Содействовать устойчивой модели использования открытого кода через существующие инструменты: разработать рекомендации по монетизации при поддержке Минцифры РФ и отраслевых сообществ, интегрировав их в программы цифровой экономики; стимулировать участие бизнеса в финансировании открытого ПО через налоговые льготы или гранты на базе платформ госуслуг; усилить защиту прав разработчиков, уточнив лицензионные нормы в рамках текущего законодательства.
2.1 Использование открытого кода связано с рисками из-за отсутствия ответственности владельцев лицензий и сложности контроля изменений, что может негативно сказаться на безопасности и стабильности продуктов компаний в условиях недостаточной прозрачности и регулирования.	2.1 Снизить риски через интеграцию существующих подходов: рекомендовать использование стабильных, проверенных версий Open Source ПО, сертифицированных по стандартам ИБ, с доступом через государственные или отраслевые реестры; внедрить технологии блокчейн для защиты интеллектуальных прав и отслеживания изменений в ПО и базах данных, присваивая уникальные идентификаторы новым версиям, на базе существующей инфраструктуры, с учетом текущих разработок в области цифровой экономики.
3.1 Проблема невозможности достижения абсолютного цифрового суверенитета при использовании ПО с открытым исходным кодом.	3.1. Обеспечить баланс безопасности и инноваций через текущие меры: ограничить применение Open Source в критических государственных сферах, заменив его сертифицированными решениями, соответствующими стандартам. 3.2. Разработать механизмы поддержки локального сообщества разработчиков через гранты и программы цифровой экономики, поощряя вклад в Open Source и создание собственных продуктов. 3.3. Использовать Open Source как основу для импортозамещения, развивая независимые ИТ-решения на национальной базе, что укрепит цифровой суверенитет.
4.1 Ограничения GPL-лицензии, обязывающей использовать ту же лицензию для производного кода, создают барьеры для разработчиков, стремящихся сохранить контроль над своими проектами или интегрировать их в экосистемы с иными моделями лицензирования, что тормозит инновации и свободу выбора в глобальном цифровом сообществе.	4.1 Необходимо развивать глобальные инициативы по созданию универсальных стандартов лицензирования, которые позволят разработчикам сочетать открытость с возможностью защиты своих интересов. Также стоит поощрять диалог между сообществами открытого ПО и коммерческими разработчиками, чтобы находить баланс между свободой распространения кода и правом на более широкий выбор моделей его использования, вдохновляя на участие в формировании справедливой цифровой среды.

5.1. Риски использования открытого исходного кода в условиях острой необходимости создания быстрых импортозамещенных решений. 5.2. Проблема безопасности: Открытый код может быть уязвим для атак, так как любой желающий может изучить его и найти уязвимости.	5.1 Разработка процедур дополнительного анализа безопасности ПО с открытым исходным кодом при его использовании в объектах КИИ. 5.2 Создание собственных версий критически важных Open Source проектов. 5.3. Усилить безопасность и разработать меры поддержки через проактивный подход разработчиков: внедрить систему непрерывного мониторинга и обновления Open Source ПО, в том числе с использованием автоматизированных платформ на основе ИИ.
6.1 Проблема опасности использования зарубежных репозиториях в условиях политических рисков.	6.1 Обеспечить гибкость и независимость в управлении кодом, поощряя компании к созданию собственных внутренних систем хранения и разработке на базе разнообразных платформ, включая отечественные решения. Подход включает поддержку использования кириллических доменов, российских сервисов для сайтов и аккаунтов, а также продвижение локальных репозиториях, чтобы укрепить цифровую автономию.
7.1 Проблема отсутствия быстрой и оперативной технической поддержки при использовании открытого кода <i>В случае появления проблем поддержка отсутствует, всё решается силами сообщества в рамках очереди баг-репортов и проще самому сделать пулл-реквест с исправлениями, но для этого нужно потратить ресурсы разработчика.</i>	7.1 Необходимо развивать внутренние стратегии привлечения и развития IT-отделов компании с целью создания и поддержки собственного (оригинального) кода. 7.2 Развитие биржи фриланс-разработчиков для Open Source – создание платформы для заказа срочных правок у независимых разработчиков, механизм верификации квалификации.
8.1 Проблема совместимости: Открытое программное обеспечение может не всегда быть совместимо с другими системами или программами.	8.1 Повысить совместимость через стандартизацию и поддержку: разработать единые рекомендации по интерфейсам и протоколам взаимодействия с использованием существующих стандартов, а также создать общедоступный тестовый полигон, где разработчики и компании смогут проверять совместимость решений в реальных сценариях, с поддержкой сообщества через форумы и программы сертификации.
9.1 Open Source-лицензии (GPL, Apache, MIT), ориентированные на правовые системы США и Европы, не имеют точных аналогов в законодательстве стран СНГ, что создает юридическую неопределенность и риски из-за различий в трактовке прав и обязанностей в отсутствие локальной адаптации.	9.1 Устранить неопределенность через практическую адаптацию: обеспечить перевод и локализацию популярных лицензий с разъяснением их положений на национальном уровне через консультации юристов, организованные отраслевыми ассоциациями 9.2 Разработать гибкие национальные шаблоны открытых лицензий, учитывающие местную специфику, но совместимые с международными нормами, а также выпустить методические рекомендации для юристов и разработчиков по применению и толкованию лицензий, распространяемые через платформы госуслуг или профессиональные сообщества.

Глобальный диалог и цифровая повестка

Проблема	Способ/подход к решению
1.1 Проблема отсутствия консенсуса по узконаправленным вопросам, которые волнуют отдельных участников обсуждения, из-за чего их мнение может быть не учтено	1.1 Структурировать процессы в рамках IG, повышая вовлеченность участников - разработать систему разделения участников IG по специфическим проблемам: сначала выделить узкие темы, вызывающие наибольшие разногласия, организовать голосование по ним среди затронутых сторон для поиска компромисса и взаимопонимания, затем перейти к обсуждению общих вопросов, по которым соглашение достигается проще, обеспечивая учет всех мнений
2.1 Отсутствует ясность в мониторинге участников информационного общества на предмет соблюдения правил пользования сервисами, а также четкий механизм реализации функции надзора у гражданского общества в области контента	2.1 Государство и технологические компании должны совместно создать условия для реализации механизма надзора со стороны гражданского общества, обеспечив законодательную базу (к примеру, разделение контента по категориям)
3.1 Проблема управления ИИ - одна из ключевых проблем современности, поскольку развитие технологий ставит перед человечеством новые вызовы.	3.1 Организовать серию информационных и образовательных кампаний, в том числе хакатонов, направленных на повышение осведомленности об этических дилеммах ИИ, основах безопасности и необходимости прозрачности, с целью разработки идей и прототипов для ответственного управления технологиями. 3.2. Разработать единый акт мягкого регулирования на основе анализа нормативных актов других стран: установить общие принципы, внедрить сертификацию ИИ-систем с учетом локальных особенностей, стимулируя инновации без строгих ограничений.
4.1 Проблема соотношения открытого Интернета и цифрового суверенитета государства. <i>Свободный доступ к информации сталкивается с потребностью стран контролировать данные, контент и технологии, что порождает фрагментацию сети и правовую неопределенность</i> 4.2. Проблема цифрового суверенитета и саморегулирования глобальных цифровых платформ <i>Цифровые платформы обладают правом блокирования пользователей или ограничения доступа пользователей к своим сервисам.</i>	4.1 Разработка универсального кодекса прозрачности: обязать платформы раскрывать алгоритмы фильтрации контента, позволяя государствам адаптировать их под свои законы, сохраняя базовый доступ для пользователей. 4.2. Пилотные проекты трансграничного обмена данными: запустить экспериментальные зоны, где страны тестируют совместное управление данными без потери контроля. 4.3. Введение добровольной сертификации интернет-платформ: сертифицировать компании, соблюдающие баланс между открытостью и уважением местных норм, стимулируя их через налоговые льготы или доступ к рынкам. 4.4. Установление глобальных принципов минимальной открытости: договориться о базовых стандартах доступа к информации (научные данные, образование), которые не подлежат ограничению, оставляя остальной контроль за государствами. 4.5. Нарастивание активности усилий по разработке международных норм и стандартов, регулирующих деятельность цифровых платформ, с учетом интересов государств, пользователей и технологических компаний. <i>В некоторых случаях возможно создание и развитие национальных и региональных цифровых</i>

	<i>платформ-альтернатив, функционирующих в соответствии с национальными интересами и требованиями.</i>
5.1 Проблема прозрачности технологических компаний в рамках межгосударственного цифрового сотрудничества	5.1 Организация системного диалога с технологическими компаниями: формулирование понятных регуляторных правил для выстраивания организациями четкой модели поведения по вопросам сбора, хранения и раскрытия данных, а также для реализации требуемых условий подотчетности, приемлемых для всех.

Цифровая деструктивность	
Проблема	Способ/подход к решению
1.1 Влияние когнитивной перегрузки на пользователя: избыточная информация (постоянный поток новостей, постоянные уведомления), параллельное выполнение задач, стресс и тревога, сжатые сроки выполнения задач (неэффективные методы работы)	1.1 Запустить государственную программу обучения продуктивности: субсидировать курсы по управлению временем и цифровыми инструментами для граждан и бизнеса, а также рассмотреть возможность включения подобных практик в образовательные организации различного уровня 1.2 Пользователям необходимо освоить различные способы разгрузки: фильтрация информации, установка приоритетов при работе с данными, частичное делегирование задач, концентрация на самой важной задаче, применение коротких медитативных практик, разделение задач на подзадачи и детальное планирование
2.1 Сложности организации цифровой детоксикации: зависимость от новых технологий, социальное давление как страх упустить что-то важное, постоянная необходимость применения технологий коммуникации в рамках работы и обучения.	2.1 Поддержка и развитие инфраструктуры офлайн-коммуникации: субсидировать библиотеки, коворкинги и общественные центры как альтернативы цифровым каналам для учебы и работы <i>На базе подобных площадок возможно проводить образовательные кампании по развитию устойчивых навыков осознанного использования технологий и устройств</i> 2.2 Изменять подходы и методы, используемые при работе с современными технологиями: замена и поиск новых привычек с введением часов «отдыха» от устройств, выработка осознанности при работе с технологиями, установление границ для противодействия социальному давлению, развитие критического мышления при потреблении контента, оптимизация использования цифровых технологий, выработка гибкого подхода к работе и учебе.
3.1 Зависимость от социальных сетей как механизма ухода от реальности, обусловленная эскапизмом, поиском внешнего одобрения, страхом одиночества и стремлением к созданию идеализированного образа, что усиливает психологическую уязвимость и подрывает ментальное благополучие общества на глобальном уровне. 3.2. Зависимость общества от цифровых сервисов, управляемых коммерческими организациями и технологическими компаниями, которые извлекают выгоду из увеличения экранного времени пользователей, стимулируя такую зависимость, что делает изменение ситуации экономически невыгодным для них.	3.1 В целях формирования осознанного подхода к использованию технологий предлагается на пользовательском уровне: ограничение времени в социальных сетях, увеличение внимания к личному общению и офлайн-взаимодействию для укрепления социальных связей, переориентация ресурсов на саморазвитие через образовательные и творческие активности, а также обеспечение доступности психологической поддержки для развития эмоциональной устойчивости. 3.2. Развитие отечественных приложений и расширений браузеров, направленных на отслеживание и ограничение времени, проводимого на определенных сайтах, в том числе в соцсетях, а также установление самоограничения на пребывание на различных сайтах, либо возможность организации устанавливать лимиты или запрет на использование соцсетей в рабочее время. 3.3. Развитие альтернативных способов формирования социальных связей вне виртуальной среды (спортивные мероприятия, культурные события, волонтерские проекты), для чего требуется поддержка развития инфраструктуры для досуга и отдыха, доступной для всех слоев населения.

	Также эффективными могут быть социальные опросы, направленные на выявления причин чрезмерного пребывания в социальных сетях, для выработки действенных и точечных механизмов решения проблемы.
4.1 Проблема отчуждения в цифровом мире. 4.2. Проблема поддержки стабильного психоэмоционального состояния в цифровом пространстве, профилактика психических расстройств, которые могут быть вызваны чрезмерным пребыванием пользователя в сети Интернет.	4.1 Повышение осведомленности о данной проблеме через информационные кампании, стимулирование реального общения посредством флешмобов по сокращению экранного времени, а также создание на государственном уровне молодежной среды, ориентированной на развитие реального взаимодействия и укрепление социальных связей. 4.2 Стимулирование проведения исследований для понимания долгосрочного влияния цифровых сервисов на психическое здоровье. Создание систем для отслеживания психоэмоционального состояния пользователей и своевременного вмешательства. 4.3 Продвижение идей баланса между онлайн и офлайн активностями через СМИ и образовательные программы. 4.4 Внедрение в систему образования предметов, посвящённых цифровой гигиене: правилам работы с информацией, защите личных данных, оптимальному использованию социальных сетей, профилактике цифровой зависимости, когнитивных перегрузок.
5.1 Проблема уязвимости человеческой психологии перед профессиональным воздействием мошенников в цифровой среде.	5.1 Выработка цифрового иммунитета через работу над собой: развитие навыков критического мышления, повышение уровня осознанности своих действий, тренировки по повышению общей концентрации внимания 5.2 Усиление существующего механизма информирования граждан, особенно наиболее уязвимых к мошенническим манипуляциям, расширение охвата через информационные потоки, увеличение частоты предупреждений, постоянная актуализация информационных сообщений дополнением их конкретными практическими шагами по распознаванию мошеннических действий и защиты.
6.1 Проблема соблюдения этичности при работе в интернете заключается в том, что не все пользователи придерживаются общих норм уважительного и ответственного поведения, а само понятие этики остается субъективным, различаясь в восприятии каждого человека, что затрудняет установление единых правил взаимодействия в цифровой среде.	6.1 Разработка и внедрение гибких норм и рекомендаций, способствующих формированию более безопасной и этичной онлайн-среды, с учетом баланса между регулированием и сохранением свободы пользователей. Стимулирование этичного поведения среди пользователей путем прозрачной модерации контента, а также реализации образовательных инициатив. 6.2. Необходимо нарастить усилия в части использования механизмов регулирования мягким правом, также возможна разработка этического кодекса поведения в цифровом пространстве. <i>В то же время принятие иных норм и законов нецелесообразно в связи с быстрыми изменениями такого пространства, а предусмотренные составы правонарушений в нормах УК РФ и КоАП охватывают нарушения в части поведения пользователей.</i>

	6.3 Рассмотрение возможности внедрения системы поощрений для лидеров мнений и/или влиятельных лиц, демонстрирующих правильное поведение в Интернет-среде. 6.4 Проведение общественных мероприятий, направленных на распространение/продвижение сетевого этикета, и потенциальная разработка технологий и механизмов, позволяющих не только фильтровать неэтичный контент, но и в перспективе выявлять конфликтогенную среду и конфликтогенную виртуальную личность.
--	---

При разработке молодежных тезисов участники Спецкурса акцентировали внимание на важности практических поведенческих рекомендаций и развития навыков, поскольку меры фискального либо технического регулирования цифровых сервисов следует признать особенно сложно реализуемыми вследствие коммерческого характера сервисов как продуктов рынка и охраняемого государством принципа свободы предпринимательства.

При таких условиях возможно предположить, что эффективными мерами могут быть организационные, которые сосредоточены на формировании культуры осознанного потребления технологий, однако данная задача также длительного времени и значительных усилий.

Цифровая дезинформация и медиаэффекты	
Проблема	Способ/подход к решению
1.1 Проблема отсутствия эффективных механизмов проверки информации затрудняет доступ пользователей к качественным данным, поскольку недостаток контроля и модерации, а также анонимность источников создают сложности в управлении информацией и снижают ее достоверность, негативно влияя на восприятие контента. 1.2. Проблема качества и достоверности информации как следствие того, что у каждого пользователя сети появилась возможность стать распространителем контента и социально значимых новостей. (Юлия Стрелец) <i>Децентрализованный тип распространения информации не является проблемой</i> 1.3. Проблема использования дипфейков при создании контента в интернете и других информационных источниках заключается в угрозе дезинформации, подрыва доверия к медиа и нарушения личной приватности.	1.1 Развитие систем для проверки фактов, автоматизация проверки данных с использованием ИИ, балансировка анонимности и ответственности при размещении каких-либо данных, применение систем фильтрации и оценки контента для качества информации. <i>Отдельными вызовами для реализации данного подхода является решение вопроса о характере подобных проектов (публичный или частный), а также обеспечения вычислительных мощностей для мониторинга массивов информации.</i> 1.2. Развитие и расширение существующих программ кибергигиены в части реализации направления повышения осведомленности пользователей и совершенствование навыков проверки информации. 1.3. Введение маркировки аккаунтов/каналов пользователей в зависимости от преобладающего характера их контента, подтверждения квалификации, рода деятельности, если планируется ввести не личный контент (развлекательный, научный, коммерческий, политический, экспертный). При этом такая маркировка должна отражаться при опубликовании каждого информационного сообщения в СМИ. 1.4. Создание механизма маркировки контента, созданного ИИ, по аналогии с зарубежными юрисдикциями, что позволит потребителям четко различать сгенерированный ИИ контент.
2.1 Проблема феномена постправды заключается в том, что истина формируется под влиянием эмоций от информации, а не объективных данных, что усиливает эмоциональную аргументацию в медиа и размывает восприятие реальности.	2.1 Ограничение доступа несовершеннолетних к соц.сетям до определенного возраста, до этого момента вводить в образовательные программы занятия, направленные на развитие критического мышления, продвижение аналитического подхода вместо эмоционального восприятия и медиаграмотности. 2.2 Разработка и внедрение этических стандартов для блогеров и лидеров мнений помогут повысить ответственность за распространение информации.
3.1 Снижение уровня коммуникации в обществе вследствие фрагментации медиапространства, где узкоспециализированные каналы вытесняют общие СМИ, ограничивая общие темы для обсуждения.	3.1. Проведение и популяризация кросс-функциональных мероприятий, очных и дистанционных, совместный обсуждений, объединяющих специалистов из разных сфер для обмена мнениями, результатами исследований единого предмета исследования, организация проектов-коллабораций факультетов в образовательных учреждениях, включение в школьные программы семинаров, на которых демонстрируется общность объекта исследований у разных предметов. 3.2 Преодоление проблемы низкого коммуникационного потенциала пользователей цифровой среды через повышение уровня социальной активности, снижение информационной перегрузки представителей данной социальной группы.

	<i>В качестве прямых действий по решению данной проблемы можно предложить:</i> - внедрение курсов, учебных дисциплин, направленных на развитие навыков поиска, анализа, обработки информации в интернет-среде, повышения навыков критического мышления с целью формирования более осознанного подхода к выбору СМИ; - оптимизацию деятельности социального института образования в направлении повышения коммуникационного потенциала обучающихся, развития «мягких» навыков. 3.3 Необходимость популяризации молодёжного туризма (создание доступных программ), поскольку туризм является сильным рычагом социализации молодёжи.
4.1 Снижение доверия социальным СМИ. 4.2 Недоверие в целом любому источнику информации, общая усталость от проверки фактов.	4.1. Создание центрального института с собственным знаком качества, присваиваемым СМИ после верификации контента независимой комиссией, который станет индикатором достоверности для пользователей, сохраняя гибкость подхода. 4.2 Закрепить как этический принцип для распространителей контента указывать первоисточник <i>Данный принцип реализован в журналистском сообществе, видится потенциал для его тиражирования.</i> 4.3 Платформы социальных медиа могут внедрять более строгие механизмы проверки фактов, сотрудничая с независимыми организациями, чтобы оценивать достоверность распространяемого контента. Такой подход поможет пользователям получать надежные и проверенные данные, снижая поток дезинформации. 4.5 Важно повышать уровень медиаграмотности пользователей, в том числе через образовательные программы и кампании, которые будут обучать людей критическому восприятию информации, а также основам работы алгоритмов, используемых в социальных сетях. От знаний о том, как формируется контент, зависит, как его воспринимает аудитория. 4.6 Использование более прозрачных алгоритмов. Социальные медиа должны раскрывать, как работает персонализация контента и предоставлять опции для настройки своих предпочтений. 4.7 Необходимо обеспечить плюрализм мнений и равную возможность распространять информацию, в том числе для тех институтов, кто эту информацию проверяет. Обеспечить работу нескольких фактчекерских организаций, а также возможность использовать данные международных сообществ, чтобы снизить последствия когнитивных искажений.
5.1 Проблема искажения фактов через восприятие опосредованной реальности.	5.1 На пользовательском уровне важен отказ от рекомендательных технологий в новостных агрегаторах, использовав данную функцию пользователь способен управлять контентом по своему желанию, но при этом такие технологии не применяются по умолчанию. 5.2 Развитие существующих программ кибергигиены в направлении усиления медиаграмотности через образовательные курсы,

формирования представления о возможностях доступа к разнообразным источникам, популяризация проверки фактов через медиа, акции и форумы с примерами внедрения в повседневную жизнь.

5.3 В качестве подхода к решению возможно рассмотреть внедрение приложений по проверки информации средствами ИИ на страницах в браузерах

Использование искусственного интеллекта для анализа и проверки фактов. ИИ может отслеживать источники информации, выявлять недостоверные данные и предлагать проверенные альтернативы.

5.4 Развитие и поддержка платформ, которые специально разработаны для борьбы с дезинформацией. Такие платформы могут использовать алгоритмы для фильтрации недостоверных материалов и предоставления пользователям сбалансированной информации по важным вопросам.

В процессе работы над итоговыми молодежными тезисами выявлен ряд сквозных и смежных проблем

Проблема	Способ/подход к решению
1.1. Проблема разрыва между динамическим развитием интернет-технологий и профессиональной компетентности, в том числе специалистов, занимающихся правовыми вопросами	1.1. Дополнение образовательных программ гуманитарного профиля с ориентиром на общую технологическую подготовку, а также программ технического профиля с акцентом на гуманитарные аспекты, развитие и расширение существующих кросс-функциональных стратегических сессий и совместных инициатив, направленных на выстраивание плодотворной коммуникации специалистов разных сфер деятельности, предмет которых - управление интернетом.
2.1. Проблема рисков "отравленных" данных в ИИ: использование необъективных или искаженных данных при разработке систем искусственного интеллекта создает угрозу появления дискриминационных алгоритмов, что подрывает доверие к технологиям и усиливает социальные риски.	2.1 Создание национальных стандартов и поддержать международные нормы (например, AI Act), обязывающие разработчиков ИИ раскрывать информацию о данных, использованных для обучения моделей, чтобы обеспечить их объективность и исключить дискриминацию. 2.2. Развитие отечественных наборов данных для обучения систем ИИ, отвечающие требованиям законодательства РФ, чтобы снизить риски использования зарубежных данных и обеспечить их правовую чистоту.
3.1. Распространение дипфейков как инструмента социальной инженерии и мошенничества угрожает достоверности информации (дезинформация), нарушает права граждан и приводит к финансовым потерям бизнеса, усиливая уязвимости в условиях недостаточной осведомленности и защиты.	3.1. Обеспечить комплексное противодействие дипфейкам через адаптацию существующих мер: уточнить их правовой статус (определение и обязательная маркировка) и ужесточить ответственность за использование в мошенничестве какотягчающее обстоятельство с введением штрафов за нарушения. 3.2. Внедрить автоматизированные инструменты фильтрации текстового контента в Интернете для выявления подозрительных материалов на базе текущих систем мониторинга, а также усилить контроль за криминальными ресурсами и поддержать идентификацию пользователей в соцсетях через интеграцию с госуслугами, координируя усилия существующих ведомств.
4.1 Проблема искажения фактов через восприятие опосредованной реальности.	4.1 Включение в программу кибергигиены широких слоев населения отдельного направления по развития навыков критического мышления, в рамках которого возможно запустить кампанию по обучению, включая мастер-классы и онлайн-курсы осознанного взаимодействия с цифровой средой.
5.1 Массовое потребление быстрого контента снижает глубину восприятия информации, способствует поверхностному мышлению и уменьшает способность к критическому анализу.	5.1. Создание коалиции, которая разработает и продвинет открытый стандарт этического дизайна приложений, включая рекомендации по ограничению экранного времени и внедрению функций цифрового детокса, а затем инициирует диалог с коммерческими компаниями для добровольного принятия этих принципов через публичное давление и партнерства.