Экология и устойчивое развитие	
Проблема	**Способ решения**
Материалы и технологии, используемые при исследованиях по уменьшению пагубного воздействия на экологию, негативно влияют на окружающую среду при их некорректной утилизации	Требуется развитие утилизации сопутствующих исследованиям отходов – от организации мероприятий по популяризации ответственного обращения до широкого распространения пунктов утилизации и переработки отходов. При этом требуется разработка экологического стандарта по использованию методов ИИ в исследованиях
Существует проблема отсутствия баланса между гонкой в технологическом развитии и экологией, при этом зачастую компании-разработчики фокусируются исключительно на прибыли, не закладывая в процесс работки экологические риски	Необходимо соотносить разработки (в том числе систем с ИИ) с этическими и экологическими принципами, а также обращать особое внимания на последствия использования технологий, на соблюдение баланса между нарушением первичной природы и нивелированием последствий
Обучение и использование искусственных нейронных сетей приводят к значительному выбросу углекислого газа, что при массовом применении негативно влияет на окружающую среду	Необходимо разработать специализированные алгоритмы, которые будут оптимизировать процесс обучения искусственных нейронных сетей с учетом энергопотребления (использование минимально необходимых вычислительных ресурсов или эффективное их перераспределение)
Центры обработки данных (ЦОД) играют важную роль в современном мире, обеспечивая работу множества систем и приложений. Однако их деятельность оказывает негативное влияние на окружающую среду, в первую очередь за счет возрастающего энергопотребления	Переход на использование энергии из возобновляемых источников, реализация более эффективных способов охлаждения, могут способствовать уменьшению экологической нагрузки от ЦОД. Требуется направить усилия научного и технического сообществ на разработку новых подходов к управлению энергопотреблением ЦОД
Для обеспечения цифровой трансформация отраслей задействуется большое количество аппаратных решений, которые сложны для последующей утилизации или повторного использования. Объем электронных отходов растет ежегодно	Требуется повышать осведомленность общественности о проблеме электронных отходов, а также активнее способствовать ответственному потреблению. Необходимо нацеливать компании на циркулярную экономику, разработать меры поощрения для компании внедряющих в процессы этапы утилизации электронных отходов и оптимизирующих использование ресурсов
Растет объем выбросов и загрязнение окружающей среды в процессе производства цифровых устройств	Необходимы разработка и внедрение законодательства, обязывающего производителей цифровой техники предоставлять программы обязательный переработки и утилизации

Экология и устойчивое развитие	
Проблема	**Способ решения**
На сегодняшний день у компаний, использующих или производящих ИКТ решения, нет четких параметров допустимого влияния таких решений на экологию	Необходимо создание цифровой таксономии, где отдельно по каждой позиции был бы обозначен допустимый уровень выбросов в атмосферу

Управление данными и доверие	
Проблема	**Способ решения**
Относительно низкий уровень доверия населения к коммерческим организациям	Обеспечение большей прозрачности политики управления данными, а также обязательное информирование населения о способах использования данных, усиление механизмов защиты персональных данных во избежание утечек
Низкий уровень цифровой грамотности населения, в частности отсутствие понимания разницы между персональными данными (публичными) и обезличенными данными (анонимными), что может быть использовано против интересов граждан	Требуется продолжение и наращивание частоты проведения мероприятий по кибергигиене широких слоев населения. Дополнительным решением могло бы послужить создание открытой базы со строго анонимными данными и открытым исходным кодом для использования в исследованиях и разработках, в том числе по обучению ИИ, а также для повышения эффективности процессов государственного управления и здравоохранения
Проблема слабости доверенного посредничества в обмене данными по линиям граждане-государство и граждане-бизнес; необходимости поддержания высокого стандарта доверенного посредничества в B2B и B2G (G2B) Государство часто не видит для себя ценности в передаче данных коммерческим компаниям, что тормозит развитие рынка Коммерческие же компании не хотят передавать государство данные бесплатно, а также беспокоятся о защите этих данных	Продвижение инструмента Доверенного посредника как экспериментального правового режима на основе цифровой песочницы с объединенными обезличенными данными
Большая часть корпоративных данных, накапливающихся в облаках и на периферии являются неструктурированными данными, которые редко анализируются или привлекаются в рамках рабочего процесса бизнес-анализа	Для обеспечения эффективного управления жизненным циклом данных компаниям следует работать в направлении создания комплексной системы администрирования данных, определяющей роли, обязанности и стандарты качества данных
Недостаточная защита прав и интересов субъектов персональных данных при их использовании частными компаниями Субъект персональных данных сохраняет связь с данной ценностью даже после совершения обмена, что увеличивает риски	Требуется разработка и внедрение механизмов контроля за использованием данных, включая прозрачные политики обработки данных и механизмы согласования сбора и использования данных с субъектами персональных данных На платформе доверенного посредника субъект передаваемых данных может управлять ими после обмена и следить за их дальнейшим использованием

Управление данными и доверие	
Проблема	**Способ решения**
Использование ИИ в обработке больших данных сопряжено с рядом проблем, одна из которых – продуцирование дезинформации (намеренное или в результате ошибок в обучении систем)	Требуется усовершенствование механизмов контроля за работой ИИ, а также развитие систем верификации алгоритмов. При этом важную роль играют операторы таких систем, с связи с чем видится целесообразным как проведение обучения операторов, так и внедрение такого элемента в целом
Недостаток координации между заинтересованными сторонами при реализации проектов в области управления данными	Развитие площадок, механизмов координации и платформ для обмена информацией между государственными учреждениями, бизнесом и академическим сообществом

Кибербезопасность, киберпреступность и безопасность в интернете	
Проблема	**Способ решения**
Технологический процесс и инновации несут неоспоримое благо, но также сопряжены с увеличением киберугроз (рост уязвимостей), в частности возникновение новых цифровых продуктов простых в эксплуатации и широкое их распространение влекут массовых характер таких угроз	Необходимо непрерывно отслеживать уязвимости и оценивать риски внедрения цифровых продуктов, обеспечивая при этом безопасность инноваций автоматически через концепцию кибериммунитета
Широкое распространения систем на базе Интернета вещей, в том числе в сфере здравоохранения, делает такие системы привлекательной целью для кибератак. При этом не все медицинские учреждения укомплектованы штатом специалистов в сфере ИТ и информационной безопасности	Для обеспечения безопасности в сфере здравоохранения, необходимы разработки и внедрение усиленных мер защиты как отдельных устройств, подключенных в Интернет вещей, таких как дефибрилляторы и инсулиновые помпы, так и всей инфраструктуры, в том числе обеспечение расширение ИТ-отделов медицинских учреждений
В процессе длительного производства аппаратных составляющих ИКТ зачастую уделяется меньшее внимание внутреннему ПО. При этом отсутствуют надежные способы защиты от уязвимостей внутреннего ПО.	Обеспечение контроля информационной безопасности на всем жизненном цикле технологии, в том числе независимая проверка соблюдения такого мониторинга. Разработка и внедрение более надежных протоколов проверки и обновления внутреннего ПО, а также реализация систем обнаружения и предотвращение вторжений в аппаратное обеспечение
Увеличение числа киберпреступлений и распространение дезинформации с использованием технологии DeepFake	Необходимость развития цифровых платформ для оперативного выявления дезинформации и применения технологии DeepFake без необходимости применения экспертного анализа. Разработка встроенных в приложения механизмов, способных автоматически определять поддельные видеоматериалы. Создания площадок для сотрудничества между техническим сообществом и сообществом медицинских и медиа экспертов, которые могли разработать алгоритмы эффективного распознавания DeepFake и дезинформации. Введение строгих правил и мер по борьбе с распространением ложной информации на различных онлайн-платформах, включая социальные сети и видеохостинги, вплоть до введения в особенную часть уголовного закона квалифицированных составов при совершении преступления с использованием технологии

Кибербезопасность, киберпреступность и безопасность в интернете	
Проблема	**Способ решения**
	DeepFake; новых составов преступлений, связанных с манипулированием общественным мнением через распространение недостоверной информации с использованием технологии DeepFake.
Данные, находящиеся на облачных платформах хранения, становится все более уязвимыми, облачные провайдеры имеют возможность использовать данные для обучения систем с ИИ	Требуется продолжение и наращивание частоты проведения мероприятий по кибергигиене широких слоев населения, в том числе отдельных мероприятий разъяснению правил и способов резервного копирования данных на независимых электронных носителях
Темпы роста угроз, зачастую, превышают темпы развития механизмов противодействия. Новые киберугрозы требуют быстрой ответной реакции и действий на опережение, но в настоящий момент рынок труда в части специалистов в сфере информационной безопасности характеризуется недостаточным количеством таких специалистов	Необходима подготовка и переподготовка кадров, способных прогнозировать будущие угрозы и находить механизмы противодействия – требуется увеличение количества бюджетных мест в вузах на соответствующих направлениях, обязать компании взаимодействовать с вузами в части подготовки программ и организации практик. Необходимо чаще проводить закрытые хакатоны "хакеров" по выявлению уязвимостей, полученные результаты использовать для повышения уровня безопасности систем, трудоустраивать победителей хакатонов. В качестве глобальных и долгосрочных мер видится целесообразным усиливать программы по дисциплине математика/математический анализ (как школьных, так и вузов), а также популяризировать профессию специалиста в области шифровая и информационной безопасности.
Перспективы развития квантовых вычислений и создания реально функционирующих квантовых компьютеров, несут новые риски информационной безопасности	На данном этапе развития систем на основе квантовых вычислений возможно применение технологии блокчейн (а в перспективе требуется направить усилия на разработку квантового блокчейна), что позволит увеличить срок актуальности данных в блоках цепочек.
Существующие прогнозы о будущих киберугрозах являются неточными, зачастую в прогнозах упоминаются угрозы, которые наблюдаются уже сегодня	Помимо обеспечения постоянного мониторинга актуальных и перспективных киберугроз, видится целесообразным создание и расширение рабочих групп, нацеленных на проведение такого мониторинга, которые могли бы предоставлять консультации, основанными на постоянном мониторинге технологического прогресса

Кибербезопасность, киберпреступность и безопасность в интернете	
Проблема	**Способ решения**
В результате цифровизация малого и среднего бизнеса, а также стартап проектов, возникают проблемы информационной безопасности, связанные с уязвимостью разрабатываемых по индивидуального заказу систем, в частности существует проблема авторизацией пользователей (хранение паролей в открытом виде)	Требуется развитие и поддержка создания больших проектов с открытым исходным кодом, который проходит системные проверки информационной безопасности. Также видится целесообразным создание упрощенных систем-аналогов ЕСИА для частных компаний
Возрастающая популярность применения ИИ и создание ненадежных систем с ИИ несет риски информационной безопасности	Разработка протоколов проверок ИИ-решений и последующая отчетность о результатах продолжительного использования таких систем в экспериментальных условиях, в том числе рассмотрение отчетов с привлечением экспертных групп
Возрастающее количество кибератак на автоматизированные системы, атаки на ПО и IT/OT-инфраструктуру	Включение в процессы мобильных аналоговых звеньев Ситуативный отказ от полной автоматизации потенциально уязвимых элементов систем Создание Red-Team в госкорпорациях и потенциально уязвимых системообразующих хозяйствующих субъектах с государственным участием, объединение таких команд в государственное Red-Team бюро Утверждение ежегодного графика проведения плановых контролируемых атак под управлением Red-Team команд по аналогии с проверочными мероприятиями. Предполагается, что ресурсное, кадровое и организационное обеспечение таких команд и бюро будет превышать таковое у потенциальных злоумышленников, в результате чего проверочные атаки будут более качественными и приведут к вакцинации уязвимых систем.
Возрастающие риски утечки и хищения данных	Обязать крупных операторов связи хранить данные в зашифрованном формате. Для использования данных потребуется их предварительная расшифровка через специализированное ПО, которое должно быть разработано уполномоченным государственным органом. Для каждого акта расшифровки требуется аутентификация оператора в ПО через систему по модели, схожей с ЕСИА. В случае использования ПО, отличного от надлежащего, а также некорректной аутентификации, копия дешифруемых данных отравляется и становится непригодной.

Глобальное цифровое управление и сотрудничество	
Проблема	**Способ решения**
Существуют разногласия между государствами. В том числе, государствам, обладающим сегодня наибольшим контролем, не выгодно перераспределять сферы влияния. При это обостряется проблема цифрового разрыва отдельных государств.	Разработка нового формата взаимодействия между основными акторами, включенных в процессы глобального цифрового сотрудничества, при этом должны быть приняты дополнительные меры для учета интересов сторон, у которых наблюдается более сильный цифровой разрыв При этом важным является безусловная деполитизация повестки
Проблема отсутствия фокуса международного диалога: чем больше аспектов включается в обсуждение, тем шире поле для разногласий, в связи с чем тяжело принять конкретное и обязательное решение	Следование принципам инклюзивности, прозрачности и открытости механизмов выработки решений. Провозглашение данных принципов главенствующими.
Резолюции встреч в сфере управления интернетом предоставляют в большинстве своём компиляцию намеченных целей, но не решений	Стоит задуматься о том, что наличие диалога и как минимум взаимопонимания – тоже результат, учитывая контроверсию тематики управления интернетом в целом Пересмотр целеполагания существующих на данный момент институтов и мероприятий не только в направлении обсуждения актуальных вопросов и вызовов, но и для постановки конкретных реализуемых целей, а также ежегодное обсуждение конечного результата Расширение полномочий МСЭ по контролю за выполнением достигнутых договоренностей
Проблема отсутствия консенсуса по узконаправленным вопросам, которые волнуют отдельных участников обсуждения, из-за чего их мнение может быть не учтено	Выработать механизм деления участников IG по узким проблемам, чтобы они могли сначала проголосовать по ним, как наиболее сложным для нахождения компромисса, и прийти к взаимопониманию, а затем переходить к обсуждению общих проблем, по которых легче всего добиться соглашения
Государство как стейкхолдер имеет более весомый голос, нежели остальные участники диалога	Принятие решений должно происходить с приоритетом на интересы гражданского общества Доработать механизмы усиливающие роль гражданского общества в принятии решений по регулированию Интернета
Низкий уровень адаптации международных форматов управления информационными	Создание механизмов обновления и адаптации международных нормативных документов с

Глобальное цифровое управление и сотрудничество	
Проблема	**Способ решения**
технологиями к быстро меняющейся цифровой среде	учетом последних технологических тенденций и вызовов
Отсутствие четкого механизма реализации функции надзора у гражданского общества в области контента	Требуется создание условий со стороны частного сектора по реализации механизма надзора гражданским сектором при обеспечении законодательных основ (разделение категорий контента, определение понятия деструктивного контента и т.д.)

Экономика данных: международное сотрудничество и технологическое лидерство	
Проблема	**Способ решения**
Высокие затраты на цифровую трансформацию. Цифровая трансформация часто требует значительных инвестиций в технологии и обучение	Разработка стратегии цифровой трансформации, планирование бюджета на основе ROI, использование облачных сервисов и инструментов с открытым исходным кодом для сокращения затрат
Отсутствие понимания необходимости внесения изменений в процессы (цифровой трансформации) как отдельной организации, так и отраслей экономики	Увеличение индекса цифровой грамотности населения (проведение комплекса мероприятий) Локально (в рамках организации) систематическое проведение обучений и тренингов по цифровым технологиям для персонала с привлечением специалистов по цифровой трансформации
Угрозы кибербезопасности могут усилиться в процессе цифровой трансформации	Внедрение современных методов шифрования, использование средств мониторинга безопасности, обучение сотрудников безопасному использованию цифровых технологий и систематическое проведение мероприятий по проверке соблюдения правил пользовательской информационной безопасности (тренировочные фишинговые рассылки и аналогичные)
Переход на цифровые технологии обычно связан с автоматизацией ряда задач и высвобождением большого количества персонала	Обеспечений гарантий предоставления альтернативной работы тем сотрудникам, задачи которых были полностью автоматизированы Разработка программ переквалификации или повышения квалификации совместно с вузами (к примеру – разработка программ обучения на операторов информационных систем с ИИ) и проведение обучения сотрудников за счет организации Разработка механизмов отслеживания скорости увольнений на государственном уровне или уполномоченными организациями
Проблема технологического отставания и зависимости государства от зарубежных продуктов и технологий	Необходимость обеспечения цифрового лидерства государства – повышение конкурентоспособности отечественных ИТ-продуктов на мировом рынке Усиление программ развития цифровой инфраструктуры в части аппаратного обеспечения, развития системы образования,

Экономика данных: международное сотрудничество и технологическое лидерство	
Проблема	**Способ решения**
	обеспечения локализации производств как части цифрового суверенитета
Проблема низкого или среднего уровня цифровой грамотности среди специалистов с высшим образованием, что существенно замедляет рабочий процесс и цифровую трансформацию компании	Развитие цифровых навыков с помощью проверенных организацией курсов и тренингов (проведение таких мероприятий на базе организации или в вузе, при этом важно участие организации в проверке соответствия содержания требованиям организации) Повышение осведомленности о необходимости умения работать с новым инструментарием

Формирование стратегий развития искусственного интеллекта	
Проблема	**Способ решения**
Высокая скорость развития технологий ИИ и как следствие усиление цифрового неравенства государств	Международное сотрудничество должно быть направлено на отслеживание и анализ новых технологий, обеспечивая обмен информацией и ресурсами, содействуя совместным исследованиям и стандартизации, что поспособствует глобальной интеграции инноваций и повышению технологическую доступности, поддерживая развитие пользовательской цифровой инфраструктуры в отдельных государствах Обеспечение равного доступа к технологиям можно обеспечить в тесном взаимодействии с международными технологическими компаниями, желающими расширить свое присутствие на рынке
Нарушение этики научной деятельности при проведении исследований с помощью ИИ	Создание механизмов контроля и надзора за использованием ИИ в научной деятельности, включая создание этических комитетов и органов, отслеживающих соблюдение правил
Нарушение авторского права при обучении ИИ	Ужесточение ограничений на обучении ИИ Рассмотрение возможности использования принудительного лицензирования в случае если использование такого объекта интеллектуальной собственности обусловлено общественно полезными целями
Потенциальные опасности некоторых векторов развития ИИ, в частности проблема отсутствия прозрачности алгоритмов влечет за собой проблемы дискриминации, защиты персональной информации и других	Необходимо развивать кодекс этики ИИ до разработки комплекса этических стандартов и нормативов для ограничения применения ИИ во вредных целях, что предусматривает защиту личных данных и человеческого достоинства, а также гарантирует прозрачность и ответственность на всех этапах разработки и эксплуатации ИИ систем
Активное развитие технологии и внедрение систем с ИИ в перспективе могут вытеснить ряд сотрудников из рабочих процессов	Обеспечение работников гарантиями трудоустройства для выполнения смежных задач, контроля и валидации результатов работы систем с ИИ, переквалификация работников в операторов систем с ИИ
Проблема возникновения ошибок при использовании ИИ из-за несовершенства моделей	Видится применимым создание и распространение отдельных инструментов верификации (прогнозирование, моделирование, симуляции, тестирование и анализ первичных

Формирование стратегий развития искусственного интеллекта	
Проблема	**Способ решения**
	данных) и валидации данных (исключает поступление заведомо ошибочных, неполных или неточных данных). Также рекомендуется создавать рабочую/рабочие группу/группы в качестве третичного уровня проверки прогнозирования и выданных решений искусственным интеллектом (тщательная перепроверка после верификации и валидации данных)
Неравномерное развитие ИИ в разных сферах деятельности вследствие непропорционального распределения ресурсов, из-за чего некоторые сферы сильно отстают в плане технического прогресса	Привлечение специалистов, ведущих разработки в области ИИ в «отстающие сферы» (сфера социального обслуживания, образования, медицина), развитие междисциплинарных образовательных программ обучения
Европоцентричность мнения и ответов систем генеративного ИИ	Наращивание отечественных разработок, усиление мер поддержки отечественных исследований Обучение отечественных систем с помощью разных источников, не только англоязычных
ИИ помогает сделать некоторые первичные выводы, но полноценный финальный анализ на данный момент способен произвести только человек	Инвестиции в научные исследования и разработку новых алгоритмов и подходов в области искусственного интеллекта помогут улучшить его возможности и эффективность Финансирование образовательных программ и курсов для подготовки квалифицированных специалистов в области ИИ способствует наращиванию человеческого капитала, необходимого для развития и внедрения ИИ Инвестиции в техническую инфраструктуру, такую как вычислительные мощности и хранилища данных, необходимы для обучения и работы сложных ИИ-систем Финансирование проектов и партнёрств между академическими кругами, промышленностью и правительствами может способствовать обмену знаниями и ускорить инновации в ИИ

Формирование стратегий развития искусственного интеллекта	
Проблема	**Способ решения**
	Вложения в стартапы и инновационные проекты в сфере ИИ могут стимулировать разработку новаторских решений и коммерциализацию технологий

В процессе работы над итоговыми молодежными тезисами выявлен ряд сквозных и смежных проблем	
Проблема	**Способ решения**
Большое количество курсов, популярность IT приводит к большому количеству неквалифицированных специалистов, а количество высококвалифицированных специалистов с хорошей подготовкой практически не растет	Подписание договоров между вузами и большими IT компаниями о сотрудничестве – обеспечение студентов производственной практикой Привлечение к образовательному процессу действующих специалистов-практиков, как минимум для консультаций в процессе обучения и/или при подготовке и актуализации программ
Утрата коммуникативных навыков, разрыв социальных связей, рост психических заболеваний среди детей молодежи в результате увеличения времени, проводимого в сети	Развитие офлайн активностей и поощрение участия в них, популяризация участия в подобных мероприятиях Развитие сети общественных пространств для молодежи Введение возрастного ценза для неограниченного использования социальных сетей и развлекательных приложений (введения обязательного контроля времени, проводимого в сети) Развитие сети коворкингов, в которых люди смогут работать в шаговой доступности от дома, не лишаясь преимуществ дистанционной работы, но при этом находясь в социуме, поощрение такого формата работы
С развитием ИКТ усугубляется положение незащищенных уязвимых групп (детей, подростков, пожилых, людей с ОВЗ (с отклонениями в психическом развитии) от киберпреступлений	Развитие законодательства в части разработки нормативных актов, защищающих уязвимые группы (к примеру, преступления, совершенные против уязвимого гражданина должны считаться преступлениями с отягчающими обстоятельствами). Наращивание темпов совместной работы государства и коммерческих организаций, связанных с техническими инновациями для уязвимых групп, для обеспечения поддержки и разработки понятных и эффективных программ защиты. Формирование особых зон в Интернете для уязвимых групп (аналогичных доменной зоне .дети) Широкое внедрение инклюзивного подхода в цифровые продукты, контроль соответствия информационной безопасности таких продуктов