МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
«ГЛАВНЫЙ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ ЦЕНТР»

Обзор
отдельных вопросов
в области больших данных и искусственного интеллекта

V ВЫПУСК

том 2

Москва 2021

Под общей редакцией В.С. Овчинского,
доктора юридических наук,
генерал-майора милиции в отставке

Обзор отдельных вопросов в области больших данных и искусственного интеллекта.

V выпуск, 2 том.
М.: ФКУ «ГИАЦ МВД России», 2021. – 440 с.

В обзоре представлены материалы, касающиеся вопросов использования больших данных и развития искусственного интеллекта в мире. Отдельно отражены актуальные вопросы использования ИИ в правоохранительной системе.

ОГЛАВЛЕНИЕ

Новые угрозы в эпоху искусственного интеллекта 4

Основы будущей обороны 27

ИИ и война 50

ИИ и будущее национальной разведки 91

Технические таланты в правительстве 102

Ускорение инноваций в области ИИ 154

Интеллектуальная собственность 167

Стратегия конкуренции и сотрудничества 197

Защита технологии 299

Модели международной инициативы по цифровой демократии 314

Содействие прозрачности и подотчетности посредством экспортного контроля 329

Благоприятный международный технологический порядок 393

Сопутствующие технологии 408

Новые угрозы в эпоху искусственного интеллекта

Социальный уровень конфликта

Информационные операции с поддержкой искусственного интеллекта. Сбор данных и Таргетинг на отдельных лиц. Состязательный ИИ. Ускоренные кибератаки. Биотехнология с поддержкой ИИ.

Правительство США не готово защищать Соединённые Штаты в наступающей эре искусственного интеллекта (ИИ). Приложения искусственного интеллекта трансформируют существующие угрозы, создают новые классы угроз и ещё больше подталкивают государственных и негосударственных противников к использованию уязвимостей в нашем открытом обществе.

Системы искусственного интеллекта расширят радиус действия и охват противников в Соединённых Штатах точно так же, как ракетный век и терроризм приблизили угрозы к дому. Благодаря ИИ противники смогут действовать с микроточностью, но в макромасштабе и с большей скоростью. Они будут использовать искусственный интеллект для усиления кибератак и кампаний цифровой дезинформации, а также для новых целей. ИИ также поможет создавать точно сконструированные биологические агенты.

А противники будут манипулировать системами искусственного интеллекта, на которые мы будем полагаться.

Как ИИ трансформирует ландшафт угроз

Современные угрозы, выдвигаемые Системами ИИ	Новые угрозы от систем ИИ	Угрозы ДЛЯ самих стеков ИИ	Будущие угрозы С ПОМОЩЬЮ систем ИИ
ИИ трансформирует существующий диапазон и охват угроз Самовоспроизводящаяся вредоносная программа, генерируемая ИИ Усовершенствованные и автономные кампании по дезинформации ИИ-инженерные и целевые патогены	ИИ создаёт новые опасные явления Глубокие фальшивки и вычислительная пропаганда Микро-Таргетинг: ИИ-слитые данные для таргетинга или шантажа Рои ИИ и нано-рои	ИИ сам по себе также является новой поверхностью атаки Атака ИИ включает в себя весь «стек ИИ». Примеры включают в себя: Инверсия модели Манипуляция обучающими данными Отравление «Озером данных»	Примеры потенциальных угроз, которые следует иметь в виду, быстрая эскалация от машины к машине с помощью автоматизированного C2 Аугментация человека с помощью искусственного интеллекта конкурентами-сверстниками Распространение простого смертоносного автономного оружия среди террористов

Технологии искусственного интеллекта усугубляют две существующие проблемы национальной безопасности:

Во-первых, цифровая зависимость во всех сферах жизни повышает уязвимость к кибератакам во всех сегментах нашего общества: корпорациях, университетах, правительстве, частных организациях и домах отдельных граждан. Параллельно в современный мир хлынули новые сенсоры. Интернет вещей (IoT), автомобили, телефоны, дома и платформы социальных сетей собирают потоки данных, которые затем могут быть переданы в системы искусственного интеллекта, которые могут идентифицировать, нацеливать, манипулировать или принуждать наших граждан.

Во-вторых, государственные и негосударственные противники бросают вызов Соединённым Штатам ниже порога прямой военной конфронтации, используя кибератаки, шпионаж, психологическую и политическую войну и финансовые инструменты. Противники не нуждаются в ИИ для проведения широкомасштабных кибератак, эксфильтрации секретных данных об американских гражданах, вмешательства в наши выборы или бомбардировки нас вредоносной информацией на цифровых платформах. Однако ИИ начинает менять эти атаки по характеру и степени, создавая новые угрозы для США. экономика, критическая инфраструктура и социальная сплоченность. Более того, эти возможности ИИ будут использоваться во всем спектре конфликтов. Они будут использоваться в качестве средств первой помощи в невоенных конфликтах, в качестве прелюдии к военным действиям или совместно с военными действиями в войне.

Американцы осознают некоторые последствия своей цифровой зависимости для конфиденциальности и потенциальные угрозы от вредоносной информации, основанной на искусственном интеллекте, такие как глубокие подделки.

Однако дебаты в Соединённых Штатах ещё не дали полного представления о масштабах и опасности угроз с использованием искусственного интеллекта и общих угрозах безопасности для систем искусственного интеллекта вокруг нас.

Перспектива использования противниками машинного обучения (МТ), планирования и оптимизации для создания систем, позволяющих манипулировать убеждениями и поведением граждан незаметными способами, – это надвигающаяся буря.

Наиболее тревожной является перспектива того, что противники будут использовать ИИ для создания оружия массового влияния, которое будет использоваться в качестве рычага во время будущих войн, в которых каждый гражданин и организация станут потенциальной мишенью.

«Больше всего беспокоит перспектива того, что противники будут использовать ИИ для создания оружия массового влияния, чтобы использовать его в качестве рычага во время будущих войн, в которых каждый гражданин и организация становятся потенциальной мишенью».

Остальная часть этой главы посвящена пяти связанным с ИИ угрозам, которые уже были или скоро будут разработаны и использованы против Соединённых Штатов.

1. Информационные операции с поддержкой искусственного интеллекта.

ИИ и связанные с ним технологии увеличат масштаб, точность и устойчивость состязательных информационных операций. ИИ усугубляет проблему злокачественной информации тремя способами:

Сообщение. ИИ может создавать оригинальный текстовый контент и манипулировать изображениями, аудио и видео, в том числе с помощью генеративной состязательной сети (GAN) и глубокого обучения подкреплению (RL), которые будет очень трудно отличить от подлинных сообщений.

Аудитория. ИИ может создавать профили предпочтений, поведения и убеждений людей, чтобы ориентироваться на конкретную аудиторию с помощью конкретных сообщений.

Средний. ИИ может быть встроен в платформы, например, с помощью алгоритмов ранжирования, для распространения вредоносной информации.

Злонамеренные информационные кампании с поддержкой искусственного интеллекта не будут просто посылать одно мощное сообщение 1 миллиону человек, как пропаганда 20-го века. Они также будут посылать миллион индивидуальных сообщений, настроенных на основе детального понимания цифровой жизни целей, эмоциональных состояний и социальных сетей.

Конкурирующие государства уже используют вредоносную информацию, используемую ИИ. Например, по данным тайваньских властей, китайское правительство проверило свои информационные возможности на основе искусственного интеллекта во время тайваньских выборов 2020 года.

Генеральный менеджер Национальной баскетбольной ассоциации подвергся преследованиям в социальных сетях за поддержку протестующих в Гонконге, в попытке которых, возможно, были задействованы автономные боты. Другие методы полагаются на созданные искусственным интеллектом поддельные персонажи. Контроль и манипулирование цифровой информацией стали центральным элементом стратегии Кремля, в том числе в попытках подорвать целостность демократического процесса в США и других странах.

В Соединённых Штатах частный сектор взял на себя ведущую роль в борьбе с иностранной вредоносной информацией. В частности, компании социальных сетей проводят обширные операции по отслеживанию и управлению информацией на своих платформах.

Но координация между правительством и фирмами социальных сетей остаётся разовой. Нам нужен более комплексный государственно-частный ответ на проблему дезинформации иностранного происхождения. Кроме того, правительство должно уделять больше внимания и ресурсов техническим проблемам обнаружения, атрибуции и аутентификации средств массовой информации. Правительство должно:

Создать Совместную межведомственную оперативную группу и Оперативный центр. Конгресс санкционировал создание Центра реагирования на иностранное пагубное влияние в рамках Управления директора национальной разведки (ODNI).

Правительство должно использовать эти полномочия для создания технологически продвинутой 24-часовой целевой группы и оперативного центра для руководства и интеграции усилий правительства по противодействию вредоносной информации из-за рубежа. Он будет изучать ландшафт соответствующих государственных и частных субъектов, координировать их действия и действовать в режиме реального времени для противодействия иностранным информационным кампаниям.

Для эффективного выявления, атрибуции и реагирования центр должен быть оснащён современными цифровыми инструментами с поддержкой искусственного интеллекта и персоналом со специализированными знаниями.

Финансировать Агентство перспективных оборонных исследовательских проектов (DARPA) для координации многочисленных исследовательских программ по обнаружению, атрибуции и разрушению вредоносных информационных кампаний с использованием искусственного интеллекта, а также для проверки подлинности происхождения цифровых медиа. Дополнительное финансирование позволит расширить текущие исследовательские программы DARPA по выявлению синтетических носителей и расширить его усилия по атрибуции и срыву вредоносных информационных кампаний. Однако перспективными могут оказаться некоторые из этих технологий обнаружения по отдельности, финансирование разработки альтернативных технологий для проверки подлинности происхождения цифровых носителей обеспечит более технологически надёжные средства предотвращения олицетворения надежных источников информации.

DARPA должно продолжать эти программы и помогать передавать все эти технологии и приложения правительственным ведомствам и агентствам, чтобы помочь в обнаружении, атрибуции и разрушении вредоносных информационных кампаний в режиме реального времени.

Создать целевую группу для изучения использования ИИ и дополнительных технологий, включая разработку и внедрение стандартов и технологий, для подтверждения подлинности и происхождения контента. Управление научно-технической политики Белого дома должно взять на себя ведущую роль в создании этой целевой группы. В ответ на проблемы дезинформации предпринимаются усилия по разработке стандартов и трубопроводов, направленных на сертификацию подлинности и происхождения аудиовизуального контента.

В этих усилиях используются технологии, включая шифрование и хрупкие водяные знаки, для обеспечения безопасности и отслеживания

ожидаемых преобразований контента по производственным и передающим трубопроводам. Эти усилия дают возможность смягчить пагубные информационные кампании, направленные на коррумпирование или подделку высоконадёжных источников информации в нашей цифровой экосистеме. Это технологическое направление созрело для государственно-частного партнёрства. Несколько частных организаций уже формируются для борьбы с дезинформацией в этой сфере.

2. Сбор данных и Таргетинг на отдельных лиц.

«Потенциальные противники узнают то, что знает каждый рекламодатель и компания социальных сетей: ИИ-это мощный инструмент таргетинга.»

Безопасность — данных-это проблема национальной безопасности.

«Ad-tech» стал «natsec-tech». Потенциальные противники узнают то, что знает каждый рекламодатель и компания социальных сетей: ИИ-это мощный инструмент таргетинга. Точно так же, как ИИ-аналитика трансформировала отношения между компаниями и потребителями, теперь она трансформирует отношения между правительствами и отдельными людьми.

Широкое распространение персональных данных стимулирует коммерческие инновации, но также создаёт уязвимости. Мы опасаемся, что систематические усилия противников по сбору данных о США компании, частные лица и правительство-это нечто большее, чем традиционный шпионаж. Противники будут комбинировать широко доступные коммерческие данные с данными, полученными незаконным путём как в 2015 году Office of Personnel Management hack для отслеживания, манипулирования и принуждения отдельных лиц. Например, инструменты, которые Китай использует для мониторинга, контроля и принуждения своих граждан, аналитика больших данных, слежка и пропаганда могут быть расширены за пределы его границ и направлены на иностранцев.

Без адекватной защиты данных ИИ затрудняет любому человеку скрытие своего финансового положения, паттерны повседневной жизни, отношений, здоровья и даже эмоций. Личные и коммерческие уязвимости становятся

слабостями национальной безопасности, поскольку противники отображают отдельных людей, сети и социальные трещины в обществе; предсказывают реакции на различные стимулы; и моделируют, как лучше манипулировать поведением или причинять вред. Появление и распространение этих методов представляет собой серьёзную проблему для контрразведки.

Для того чтобы правительство рассматривало данные своих граждан и предприятий как актив национальной безопасности, необходимы существенные изменения в том, как мы думаем о безопасности данных, а также в нашей политике и законах, направленных на её укрепление.

Нам необходимо определить категории и комбинации личных и коммерческих данных, которые являются наиболее чувствительными. Первые попытки ограничить сбор данных иностранными противниками, например, решение правительства заставить китайскую компанию отказаться от владения популярным приложением знакомств из-за страха того, что враждебный противник может сделать с конфиденциальными частными данными, представляют собой важные начальные шаги.

Однако правительству не хватает широкого подхода с чёткой политикой, критериями или полномочиями для решения этой многогранной проблемы. Правительство должно:

Разработка политики, рассматривающей безопасность данных как национальную безопасность, в том числе в этих областях:

Во-первых, с технической точки зрения правительство должно обеспечить, чтобы для его собственных систем искусственного интеллекта (включая приобретаемые им коммерческие системы) существовал подход жизненного цикла разработки безопасности, который должен включать в себя акцент на потенциальных атаках на конфиденциальность.

Red teaming должен включать в себя опыт конфиденциальности. Государственные базы данных должны быть объединены и анонимизированы, когда это возможно, а личные данные должны храниться не дольше, чем это

необходимо, чтобы затруднить противникам использование информации в злонамеренных целях.

Во-вторых, правительство должно обеспечить, чтобы конфиденциальность и безопасность данных были приоритетными соображениями в рамках более широких усилий по усилению контроля за иностранными инвестициями, а также разведки цепочек поставок и управления рисками.

В-третьих, национальные усилия по законотворчеству и регулированию защиты данных и конфиденциальности должны учитывать соображения национальной безопасности, такие как ограничение способности враждебных иностранных субъектов приобретать конфиденциальные данные об американцах на коммерческом рынке.

3. Ускоренные Кибератаки.

Вредоносное ПО в эпоху искусственного интеллекта сможет мутировать в тысячи различных форм, как только оно попадёт в компьютерную систему. Такие мутирующие полиморфные вредоносные программы уже составляют более 90% вредоносных исполняемых файлов. Глубокие инструменты RL уже могут находить уязвимости, скрывать вредоносные программы и атаковать выборочно. Хотя неясно, какие методы будут доминировать, существует чёткий путь для США. противники трансформируют эффективность кибератак и шпионских кампаний с помощью ансамбля новых и старых алгоритмических средств автоматизации, оптимизации и информирования атак. Это выходит за рамки вредоносного ПО с улучшенным ИИ. Машинное обучение имеет текущие и потенциальные приложения на всех этапах кампаний кибератак

«Машинное обучение имеет текущие и потенциальные приложения на всех этапах кампаний кибератак» и изменит природу кибервойны и киберпреступности, существующие кибер-возможности ИИ сделают кибератаки более точными и адаптированными. Расширяющееся применение ещё больше ускорит и автоматизирует кибервойну, позволит использовать

более скрытное и стойкое кибероружие и сделает кибератаки более эффективными в более широком масштабе.

Оборона США оказалась неспособной справиться с ещё более элементарными киберпространственными вызовами. Уязвимости остаются открытыми в устаревшей инфраструктуре и медицинских устройствах, в то время как новые уязвимости распространяются в сетях 5G, миллиардах устройств IoT и в цепочках поставок программного обеспечения. Многомиллиардный глобальный ущерб, нанесённый российской атакой NotPetya в 2017 году, конкретно демонстрирует мощь даже базовых автоматизированных вредоносных программ, толерантность к риску способных государственных субъектов и последствия распространения таких возможностей.

Хотя оборонительные приложения ИИ обещают улучшить нашу национальную киберзащиту, ИИ не может защитить изначально уязвимую цифровую инфраструктуру. Чтобы справиться с нынешней угрозой Конгресс должен продолжать выполнять рекомендации Комиссии по киберпространству.

С помощью этого фундамента для киберзащиты США могут подготовиться к расширению угроз путём тестирования и создания инструментальной инфраструктуры, необходимой для киберзащиты, создания лучших стимулов для обеспечения безопасности, правильной организации для решения проблемы и поддержания равновесия атакующих. Всепроникающий кибершпионаж и атаки на США компьютерные сети и критическая инфраструктура будут продолжаться и станут ещё более разрушительными с ИИ, если не будут приняты срочные федеральные меры. Правительство должно:

Разработка и развёртывание средств защиты от кибератак с использованием искусственного интеллекта. Агентства национальной безопасности должны приобрести датчики и приборы, необходимые для обучения систем искусственного интеллекта обнаруживать угрозы в своих сетях и реагировать на них. Киберзащита с поддержкой искусственного

интеллекта также нуждается в крупномасштабном, инструментальном и реалистичном тестировании, и она должна быть достаточно надёжной, чтобы противостоять атакам противника.

Эти средства защиты должны использоваться для расширения обмена информацией о скорости машин, обнаружения аномалий на основе поведения и смягчения последствий вредоносных программ в правительственных сетях. Чтобы извлечь выгоду из этих возможностей, правительство должно ускорить создание Совместного центра киберпланирования и операций по образцу Национального центра по борьбе с терроризмом. Центр будет выполнять функции централизованного подразделения по обмену кибератаками и сотрудничеству с межведомственной юрисдикцией и органами власти для расследования угроз, активной поддержки мер по смягчению защитных мер и координации ответных мер.

Состязательный ИИ.

Системы искусственного интеллекта представляют собой новую цель для атаки. В то время как мы находимся на переднем крае этого явления, коммерческие фирмы и исследователи задокументировали атаки, которые включают в себя уклонение, отравление данных, репликацию моделей и использование традиционных программных недостатков для обмана, манипулирования, компрометации и неэффективности систем ИИ.Эта угроза связана с традиционной кибернетической деятельностью, но отличается от неё, поскольку системы ИИ будут уязвимы для враждебных атак из любой области, где ИИ усиливает действия гражданские или военные. Учитывая зависимость систем ИИ от больших наборов данных и алгоритмов, даже небольшие манипуляции с этими наборами данных или алгоритмами могут привести к последовательным изменениям в том, как работают системы ИИ. Угроза не является гипотетической: враждебные атаки происходят и уже влияют на коммерческие системы ML. За редкими исключениями, идея защиты систем ИИ была запоздалой мыслью в разработке и внедрении систем ИИ при недостаточных инвестициях в исследования и разработки. Только три из 28

недавно опрошенных организаций имеют «правильные инструменты для обеспечения безопасности своих систем ОД».

До сих пор не было предпринято единообразных усилий по интеграции обеспечения ИИ во все предприятия национальной безопасности США. Чтобы улучшить «уверенность» ИИ, правительство должно:

Создайте Национальную систему обеспечения ИИ. Все правительственные учреждения должны будут разработать и применить систему состязательных угроз мл для решения вопроса о том, как ключевые системы ИИ могут быть атакованы и должны быть защищены. Аналитическая структура может помочь классифицировать угрозы правительственным системам искусственного интеллекта и помочь аналитикам в обнаружении, реагировании и устранении угроз и уязвимостей.

Создайте специальные красные команды для состязательного тестирования. Красные команды должны занять наступательную позицию, пытаясь сломать системы и заставить их нарушать правила соответствующего поведения. Из-за нехватки необходимых знаний и опыта для команд AI red Минобороны и ODNI должны рассмотреть вопрос о создании общегосударственных сообществ возможностей AI red-teaming, которые могли бы быть применены к многочисленным разработкам AI.

5. Биотехнология с поддержкой искусственного интеллекта.

Биология теперь программируется. Новые технологии, такие как инструмент редактирования генов CRISPR, открыли эру, когда люди могут редактировать ДНК. В сочетании с мощными вычислительными мощностями и искусственным интеллектом инновации в биотехнологии могут обеспечить новые решения для самых неприятных проблем человечества, в том числе в области здравоохранения, производства продуктов питания и экологической устойчивости. Однако, как и другие мощные технологии, применение биотехнологий может иметь и тёмную сторону. Пандемия COVID-19 напомнила миру об опасности очень заразного патогена. ИИ может позволить патогену быть специально сконструированным для летальности или

нацеленным на генетический профиль, конечное оружие дальности и досягаемости. Кроме того, ИИ, применённый к биологии, может оптимизировать физиологическое развитие человека, включая интеллект и физические характеристики. В той мере, в какой мозговые волны могут быть представлены как вызов машинного зрения для ИИ, тайны мозга могут быть раскрыты и запрограммированы.

Отдельные люди, общества и государства будут иметь различные моральные и этические взгляды и принимать различные степени риска во имя прогресса, и американские конкуренты, сравнительно вероятно, предпримут более терпимые к риску действия и будут менее жёстко соответствовать биоэтическим нормам и стандартам.

Китай понимает огромный потенциал, связанный с руководством биологической революцией. Массивные наборы геномных данных в таких местах, как BGI Group (ранее известный как Пекинский институт геномики), в сочетании с ныне глобальной платформой сбора генетических данных Китая и «общенациональным» подходом к ИИ, сделают их грозным конкурентом в области биологии. BGI может служить, вольно или невольно, глобальным механизмом сбора генетических баз данных китайского правительства, предоставление Китаю большего количества необработанных и разнообразных образцов генома человека, а также доступа к конфиденциальной личной информации о ключевых лицах по всему миру.

Соединённые Штаты не могут позволить себе оглянуться назад через 10 лет и «удивиться» биотехнологическому эквиваленту Huawei.

Кроме того, давнее пренебрежение Россией научными нормами и биоэтическими принципами, продемонстрированное её разработкой и использованием новых нервно-паралитических веществ, таких как «Новичок», для покушений на убийство вызвало озабоченность Правительства США по поводу соблюдения Россией Конвенции о биологическом оружии, что может предвещать готовность использовать передовые биотехнологические возможности в гнусных целях.

Правительство должно:

Повысить значимость вопросов биобезопасности и биотехнологии в органах национальной безопасности США. Учитывая, как ИИ существенно увеличит темпы технического прогресса в биотехнологии, правительству следует обновить Национальную стратегию биологической защиты, включив в неё более широкое видение биологических угроз, таких как улучшение человеческого потенциала, использование генетических данных в злонамеренных целях и способы использования американскими конкурентами преимуществ биотехнологии или биоданных в новых целях. Кроме того, США официальные лица должны предупреждать об опасностях, связанных с получением иностранными субъектами личной генетической информации, особо подчёркивая озабоченность по поводу связей между BGI и китайским правительством.

Примечания

1 Угроза может быть понята как способность противника в сочетании с уязвимостью, которая может создать вредные последствия. Угрозы могут быть классифицированы далее по их серьезности, вероятности, неизбежности и податливости.

2 Stuart A. Thompson & Charlie Warzel, Двенадцать Миллионов телефонов, Один набор данных, Нулевая конфиденциальность, New York Times (19 декабря 2019 года), https://www.nytimes.com/interactive/2019/12/19/opinion/location-trackingcell-phone.html. Например, интернет вещей (IoT) и приложения на базе искусственного интеллекта могут превратить ваш новый робот-пылесос в подслушивающее устройство. См. Sriram Sami, et al., Spying with Your Robot Vacuum Cleaner: Eavesdropping via Lidar Sensors, Proceedings of the 18th Conference on Embedded Networked Sensor Systems (Nov. 2020), https://dl.acm.org/doi/10.1145/3384419.3430781.

3 Это в некотором смысле аналогично тому, что стратеги холодной войны называли «контрценностным таргетированием».» См. Lawrence Freedman, The Evolution of Nuclear Strategy, Palgrave Macmillan Vol. 20 at 119-122 (1989). В области ядерной стратегии это также называлось контргородским или контрэкономическим таргетированием.

4 Некоторые наблюдатели использовали понятие «острой власти» для описания таких попыток оказывать влияние в открытых обществах. Такое использование власти является острым «в том смысле, что [авторитарные государства стремятся] пронзить, проникнуть или пробить информационную среду в целевых странах.» Sharp Power: Rising Authoritarian Influence, National Endowment for Democracy at 13 (Dec. 5, 2017), https:// www.ned.org/sharp-power-rising-authoritarian-influence-forum-report/. См. Также Свидетельство доктора Эрика Хорвица, Microsoft, перед США. Сенатский комитет по торговле, науке и транспорту, Подкомитет по космосу, науке и конкурентоспособности, Слушания на Заре искусственного интеллекта в 13 (30 ноября 2016 года), http://erichorvitz.com/Senate_Testimony_Eric_Horvitz.pdf.

5 Мэтт Чессен, The MADCOM Future: Как искусственный интеллект усилит компьютерную пропаганду, перепрограммирует человеческую культуру и угрожает демократии… и Что С Этим Можно Поделать, Атлантик Совет (сентябрь 2017 года), https://www.atlanticcouncil.org/wp-content/uploads/2017/09/The_MADCOM_ Future_RW_0926.pdf.

6 Филип Шеруэлл, Китай Использует Тайвань для целевой практики ИИ, чтобы повлиять на выборы, Австралиец (5 января 2020 года), https://www.theaustralian.com.au/world/the-times/china-uses-taiwan-for-ai-target-practiceto-influence-elections/news-story/57499d2650d4d359a3857688d416d1e5.

7 Ben Cohen, et al., How One Tweet Turned Pro-China Trolls Against the NBA, Wall Street Journal (Oct. 16, 2019), https://www.wsj.com/articles/how-one-tweet-turned-pro-china-trolls-against-thenba-11571238943. Об автоматических ботах см., Например, Sarah Kreps & Miles McCain, Not Your Father's Bots, Foreign Affairs (2

августа 2019 года), https://www.foreignaffairs.com/articles/2019-08-02/not-yourfathers-bots.

8 Джеймс Винсент, Онлайн-Пропагандистская кампания, Использовавшая Сгенерированные ИИ Снимки Головы для создания Фальшивых журналистов, The Verge (7 июля 2020 года), https://www.theverge.com/2020/7/7/21315861/ai-generatedheadshots-profile-pictures-fake-journalists-daily-beast-investigation.

9 Последние исследования технических аспектов вмешательства России в выборы 2016 года см. в статье Alexander Spangher, et al., Характеризующей поисковый трафик в Интернет-исследовательском агентстве Web Properties, Web Conference (2020), https://www.microsoft.com/en-us/research/publication/characterizingsearch-engine-traffic-to-internet-research-agency-web-properties/; Ryan Boyd, et al., Характеризуя деятельность Агентства интернет-исследований в социальных сетях во время Президентских выборов в США в 2016 году С использованием лингвистического анализа, PsyArXiv Preprints (2018), https://psyarxiv.com/ajh2q/. См. также Алину Полякову, «Оружие слабых: Асимметричная война России и искусственного интеллекта», Брукингский институт (15 ноября 2018 г.), https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-drivenasymmetric-warfare/.

10 См. Pub. L. 116-92, National Defense Authorization Act for Fiscal Year 2020, 133 Stat. 1198, 2129 (2019).

11 К ним относятся программы Media Forensics (MediFor) и Semantic Forensics (SemaFor). См. Д-ра Мэтта Турека, Медиа-криминалистика, DARPA (последний доступ 10 июня 2021 года), https://www.darpa.mil/program/media-forensics; Доктор Мэтт Турек, Семантическая криминалистика, DARPA (последний доступ 10 января 2021 года), https:// www.darpa.mil/program/semantic-forensics.

12 См., Например, Paul England, et al., AMP: Authentication of Media via Provenance, arXiv (20 июня 2020 г.), https://arxiv.org/abs/2001.07886.

13 См., Например, Paul England, et al., AMP: Authentication of Media via Provenance, arXiv.

14 См. Раздел Создание стандарта атрибуции цифрового контента, Инициатива по аутентичности контента, https://contentauthenticity.org/; и Происхождение проекта: Защита доверенных носителей, Происхождение проекта, https://www.originproject.info/about.

15 Роберт Уильямс описал, как политики сталкиваются с «головоломкой инновационной безопасности», одним из аспектов которой является «беспокойство о том, что конфиденциальность данных и национальная безопасность все больше взаимосвязаны. Данные (и сети передачи данных) могут использоваться таким образом, чтобы угрожать безопасности, но они также формируют жизненную силу технологических инноваций, от которых зависят как экономический рост, так и национальная безопасность.» Роберт Д. Уильямс, Разработка многосторонней политики в области технологий и кибербезопасности, Брукингс, 1 ноября 2020 года, https://www.brookings.edu/wp-content/uploads/2020/11/Robert-D-Williams.pdf.

16 Эллен Накасима, С помощью Серии Крупных Взломов Китай создает базу данных об американцах, Washington Post (5 июня 2015 г.), https://www.washingtonpost.com/world/national-security/in-a-series-of-hackschina-appears-to-building-a-database-on-americans/2015/06/05/d2af51fa-0ba3-11e5-95fdd580f1c5d44e_story.html.

17 Другим примером того, как противник получает важные данные о физических лицах США, является взлом агентства кредитной отчетности Equifax. Пресс-релиз Министерства юстиции, Китайские военнослужащие обвиняются в компьютерном мошенничестве, экономическом шпионаже и мошенничестве с проводами за взлом Агентства кредитной отчетности Equifax (10 февраля 2020 года), https://www.justice.gov/opa/pr/chinese-military-personnel-chargedcomputer-fraud-economic-espionage-and-wire-fraud-hacking; Аруна Вишваната и др., Четыре члена китайских военных Обвиняются В массовом нарушении Equifax, Wall Street Journal (февраль. 11, 2020), https://www.wsj.com/articles/four-members-of-china-s-military-indicted-for-massive-equifaxbreach-11581346824.

18 См., Например, Дрю Харвелл и Ева Доу, Huawei Протестировали Программное Обеспечение искусственного Интеллекта, Которое Могло Бы Распознавать Уйгурские Меньшинства и Предупреждать Полицию, Говорится В отчете Washington Post (8 Декабря 2020 года). https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighurminorities-alert-police-report-says/; Хью Харсоно, Китайская технология слежки следит за населением по всему миру, The Diplomat (18 июня 2020 года), https://thediplomat.com/2020/06/chinas-surveillance-technology-is-keeping-tabs-on-populations-around-the-world/.

19 См. Джеймс Бейкер, Контрразведывательные последствия искусственного интеллекта-Часть III, Lawfare (10 октября 2018 г.), https://www.lawfareblog.com/counterintelligence-implications-artificial-intelligence-part-iii.

20 YuanYang & James Fontanella-Khan, Мясорубка, Проданная китайским владельцем После проблем национальной безопасности США, Financial Times (7 марта 2020 года), https://www.ft.com/content/a32a740a-5fb3-11ea-8033-fa40a0d65a98.

21 Об атаках на конфиденциальность см. Maria Rigaki & Sebastian Garcia, A Survey of Privacy Attacks in Machine Learning, arXiv (15 июля 2020 г.), https://arxiv.org/abs/2007.07646.

22 Комитет по иностранным инвестициям в США (CFIUS) уполномочен рассматривать сделки, включающие «конфиденциальные персональные данные граждан Соединённых Штатов, которые могут быть использованы таким образом, который угрожает национальной безопасности».» Для получения дополнительной информации см. Laura Jehl, Spotlight on Sensitive Personal Data As Foreign Investment Rules Take Force, The National Law Review (Feb. 18, 2020), https://www.natlawreview.com/article/spotlight-sensitive-personal-data-foreign-investment-rules-takeforce. Национальный центр контрразведки и безопасности (NCSC) включает «конфиденциальные правительственные данные и личную информацию» в свою концепцию ключевых рисков цепочки поставок. См.

Управление рисками цепочки поставок: Снижение угроз ключевым цепочкам поставок США, NCSC at 3 (2020), https://www.dni.gov/files/NCSC/documents/supplychain/20200925-NCSC-Supply-Chain-Risk-Managementtri-fold.pdf.

23 См., Например, Graham Webster, App Bans Won't Make U. S. Security Risks Disappear, MIT Technology Review (21 сентября 2020 г.), https://www.technologyreview.com/2020/09/21/1008620/wechat-tiktok-banchina-us-security-policy-opinion/.

24 Nicholas Duran, et al., 2018 Webroot Threat Report, Webroot at 6 (2018), https://www-cdn.webroot.com/9315/2354/6488/2018-Webroot-Threat-Report_US-ONLINE.pdf.

25 Gary J. Saavedra, et al., A Review of Machine Learning Applications in Fuzzing, arXiv (Oct. 9, 2019), https://arxiv.org/pdf/1906.11133.pdf; Исао Такаесу, Machine Learning Security: Deep Exploit, GitHub (29 августа 2019), https://github.com/13o-bbr-bbq/machine_learning_security/tree/master/DeepExploit; Марк Ph. Stoecklin, et al., Deep Locker: How AI Can Power a Stealthy New Breed of Malware, Security Intelligence (Aug. 8, 2018), https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthynew-breed-of-malware/.

26 Последствия искусственного интеллекта для кибербезопасности: Материалы семинара, Национальные академии наук, техники и медицины (2019), https://doi.org/10.17226/25488; Nektaria Kaloudi & Jingyue Li, The AI-Based Cyber Threat Landscape, ACM Computing Surveys at 1-34 (Feb. 2020), https://dl.acm.org/doi/abs/10.1145/3372823; Ben Buchanan, et al., Automating Cyber Attacks, Center for Security and Emerging Technology (Nov. 2020), https://cset.georgetown.edu/research/automating-cyber-attacks/; Dakota Cary & Daniel Cebula, Destructive Cyber Operations and Machine Learning, Center for Security and Emerging Technology at 5-23 (Nov. 2020), https://cset.georgetown.edu/research/destructive-cyber-operations-and-machine-learning/.

27 Последствия искусственного интеллекта для кибербезопасности: Материалы семинара, Национальные академии наук, техники и медицины (2019), https://doi.org/10.17226/25488.

28 Недавняя атака SolarWinds демонстрирует глубокие уязвимости в наших цепочках поставок программного обеспечения. См. Совместное заявление Федерального бюро расследований (ФБР), Агентства по кибербезопасности и инфраструктурной безопасности (CISA) и Канцелярии Директора национальной разведки (ODNI), Канцелярии Директора национальной разведки (16 декабря 2020 года). https://www.dni.gov/index.php/newsroom/pressreleases/item/2175-joint-statement-by-the-federal-bureau-of-investigation-fbi-the-cybersecurity-andinfrastructure-security-agency-cisa-and-the-office-of-the-director-of-national-intelligence-odni.

29 Последствия искусственного интеллекта для кибербезопасности: Материалы семинара, Национальные академии наук, техники и медицины (2019), https://doi.org/10.17226/25488; Ben Buchanan, et al., Automating Cyber Attacks, Center for Security and Emerging Technology at 3 (Nov. 2020), https://cset.georgetown.edu/research/automating-cyber-attacks/.

30 Отчет Комиссии по солярию киберпространства, Комиссия по солярию Киберпространства США (март 2020 года), https://www.solarium.gov/report.

31 См. Рекомендацию 5.4 в Отчете Комиссии по солярию Киберпространства США, Комиссия по солярию Киберпространства США, 87 (март 2020 года), https://www.solarium.gov/report.

32 Матрица угроз состязательного ИИ: Тематические исследования, GitHub (последний доступ 10 января 2021 года), https://github.com/mitre/advmlthreatmatrix/blob/master/pages/case-studies-page.md. Подробнее о применении состязательного ИИ см. Naveed Akhtar & Ajmal Mian, Threat of Adversarial Attacks on Deep Learning in Computer Vision: A Survey, IEEE (28 марта 2018 г.), https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8294186.

33 Состязательный ИИ - это то, что можно сделать с системами ИИ. Наука защиты и защиты приложений ИИ от атак называется «AI Assurance.» Наука о

нападении на каждый технологический компонент ИИ называется «Контр-ИИ».»

34 Ram Shankar Siva Kumar & Ann Johnson, Кибератаки На Системы Машинного Обучения Встречаются Чаще, Чем Вы Думаете, Microsoft Security (22 Октября 2020 Года), https://www.microsoft.com/security/blog/2020/10/22/cyberattacks-against-machine-learning-systems-are-more-common-thanyou-think/.

35 Было подсчитано, что менее 1% финансирования исследований и разработок в области ИИ направляется на обеспечение безопасности систем ИИ. См. Nathan Strout, The Three Major Security Threats to AI, Center for Security and Emerging Technology (10 сентября 2019), https://cset.georgetown.edu/article/the-three-major-security-threats-toai/.

36 Ram Shankar Siva Kumar, et al., Adversarial Machine Learning—Industry Perspectives, arXiv at 2 (21 мая 2020 г.), https://arxiv.org/pdf/2002.05646.pdf.

37 Существуют различные текущие государственные и частные усилия, включая, например, систему MITRE-Microsoft adversarial мл framework. См. Ram Shankar Siva Kumar & Ann Johnson, Кибератаки На Системы Машинного Обучения Встречаются Чаще, Чем Вы Думаете, Microsoft Security (22 Октября 2020 Г.), https://www.microsoft.com/security/blog/2020/10/22/cyberattacks-against-machine-learning-systemsare-more-common-than-you-think/; Матрица угроз состязательного ИИ: Тематические исследования, MITRE (последний доступ 10 января 2021 года), https://github.com/mitre/advmlthreatmatrix/blob/master/pages/case-studies-page.md.

38 Аналогичную рекомендацию см. в статье Michèle Flournoy, et al., Building Trust Through Testing, estate Advisors at 27 (Oct. 2020), https://cset.georgetown.edu/wp-content/uploads/Building-TrustThrough-Testing.pdf. (Flournoy, et al., утверждают, что «национальная команда AI и мл red является центральным центром для тестирования против состязательных атак, объединяя операторов и аналитиков Министерства обороны, исследователей ИИ, T&E [Центральное разведывательное управление (ЦРУ), Оборонное

разведывательное управление (DIA), Агентство национальной безопасности (NSA)] и другие компоненты IC, по мере необходимости. Это будет независимая объединенная организация, которая будет обладать как техническим, так и разведывательным опытом, чтобы имитировать реалистичные атаки противника в имитируемой оперативной среде.»)

39 BGI построила и управляет China National GeneBank, национальной генетической базой данных китайского правительства. Она также является крупным мировым поставщиком тестов COVID-19, которые потенциально обеспечивают доступ к крупным международным наборам генетических данных; к 30 июня 2020 года она поставила более 35 миллионов тест-наборов в 180 стран, включая Соединенные Штаты, и построила 58 тестовых лабораторий в 18 странах. См. Кирсти Нидхэм, Специальный Репортаж: COVID Открывает новые двери для китайского Генного гиганта, Reuters (Aug. 5, 2020), https://www.reuters.com/article/us-health-coronavirus-bgi-specialreport/special-report-covid-opensnew-doors-for-chinas-gene-giant-idUSKCN2511CE.

40 Джон Вертхайм, Китайское стремление контролировать будущее американского здравоохранения, 60 минут (31 января 2021 года), https://www.cbsnews.com/news/china-us-biodata-60-minutes-2021-01-28/?ftag=CNM-00-10aab7d&linkId=110169507; Кирсти Нидхэм, Специальный Репортаж: COVID Открывает новые двери для китайского Генного гиганта, Reuters (5 августа 2020 года), https://www.reuters.com/article/us-health-coronavirus-bgispecialreport/special-report-covid-opens-new-doors-for-chinas-gene-giant-idUSKCN2511CE.

41 Сэр Ричард Переспена, Что такое Новичок, российский нервно-паралитический агент, Связанный с отравлением Навального?, New York Times (2 сентября 2020 года), https://www.nytimes.com/2020/09/02/world/europe/novichok-skripal. html; 2020 Присоединение и соблюдение Соглашений и обязательств в области контроля над вооружениями, нераспространения и разоружения (Доклад о соблюдении), Государственный департамент США на Pt. V (2020), https://2017-

2021.state.gov/2020-adherence-to-and-compliance-with-arms-control-nonproliferationand-disarmament-agreements-and-commitments-compliance-report-2//index.html#_Toc43298166.

42 Дополнительные рекомендации, касающиеся взаимосвязи ИИ и биотехнологии, см. в главе 16 настоящего доклада.

Основы будущей обороны

Будущая оборона с поддержкой искусственного интеллекта

Постройте техническую основу	
Ускорить внедрение существующих цифровых технологий	Тренируйте и обучайте Бойцов
Инвестируйте в возможности следующего поколения	Демократизировать развитие ИИ

С конца холодной войны американские военные обладают военно-техническим превосходством над всеми потенциальными противниками. Теперь его техническое мастерство оспаривается, особенно Китаем и Россией. Высшее военное руководство предупредило, что если нынешние тенденции не будут изменены, то американские военные в ближайшие годы потеряют своё военно-техническое превосходство. Искусственный интеллект (ИИ) является ключевым аспектом этой проблемы, поскольку оба наших великих конкурента считают, что они смогут компенсировать наше военное преимущество с помощью систем с поддержкой ИИ и автономии с поддержкой ИИ. В ближайшие десятилетия Соединённые Штаты победят технически сложных противников только в том случае, если ускорят внедрение сенсоров и систем управления, вооружения и материально-технического обеспечения с поддержкой искусственного интеллекта.

Министерство обороны (МО) должно поставить перед собой амбициозную цель. К 2025 году должны быть заложены основы для широкой интеграции ИИ в МО.

Эти основы включают общую цифровую инфраструктуру, доступную как внутренним командам разработчиков ИИ, так и критически важным отраслевым партнёрам, цифровую грамотную рабочую силу и современные бизнес-практики с поддержкой ИИ, повышающие эффективность.

Все они являются предпосылками для достижения состояния боевой готовности ИИ, которое обсуждается в главе 3 настоящего доклада.

«К 2025 году должны быть заложены основы для широкой интеграции ИИ в МО.»

Министерство обороны сильно отстаёт от коммерческого сектора в интеграции новых и прорывных технологий, таких как ИИ, в свою деятельность.

Очаги превосходства начали появляться в 2017 году, когда был запущен проект Maven с целью упростить работу аналитиков разведки путём распознавания объектов в видеозаписях, снятых беспилотными летательными аппаратами и другими платформами.

Другие многообещающие инициативы - это тесты уровня обслуживания. Однако дальновидные технологи и военные бойцы в значительной степени остаются в тупике из-за устаревших технологий, громоздких процессов и структур стимулов, которые предназначены для устаревших или конкурирующих целей. Успех обычно основан на обходных путях-несмотря на систему.

«... дальновидные технологи и военные бойцы в значительной степени остаются в тупике из-за устаревших технологий, громоздких процессов и структур стимулов, которые предназначены для устаревших или конкурирующих целей» .

Препятствий для интеграции ИИ много.

Минобороны уже давно ориентировано на корабли, самолёты и танки. Сейчас он пытается сделать скачок к предприятию с интенсивным программным обеспечением.

Расходы по-прежнему сосредоточены на устаревших системах, разработанных для индустриальной эпохи и холодной войны. Между тем бюрократия препятствует партнёрству с технологическими фирмами и критическим усилиям по расширению инновационной базы национальной безопасности.

Перспектива бюрократических рычагов отпугивает компании от работы с Минобороны; для многих стартапов экономически нерационально даже пытаться. Традиционные оборонные компании по-прежнему будут играть центральную роль в создании и интеграции крупных систем ведения войны с использованием ИИ. Однако даже эти подрядчики, обладающие ресурсами и опытом для управления системой, сталкиваются с технологическими и техническими препятствиями, которые замедляют усилия по созданию и интеграции систем ИИ.

Многие процессы по-прежнему слишком сильно зависят от PowerPoint и ручных рабочих потоков. Данные, необходимые для подпитки машинного обучения (мл), в настоящее время перегружены, грязны или часто отбрасываются.

Платформы отключены. Методы приобретения, разработки и внедрения в основном следуют жёстким, последовательным процессам, препятствующим раннему и непрерывному экспериментированию и тестированию, критически важным для ИИ.

Даже многообещающие программы искусственного интеллекта ещё не принесли ожидаемых результатов и часто остаются привязанными к проприетарному программному обеспечению и хранилищам данных коммерческих поставщиков.

Такие шаги, как создание облачной инфраструктуры, необходимой для масштабирования приложений искусственного интеллекта, выполняются медленно. Соглашения о передаче данных и обновления программного обеспечения, которые в промышленности занимают часы или дни,

превращаются в многомесячные задержки. Служащим на всех уровнях не хватает технического образования и опыта для использования ИИ.

В результате перемены будут нелёгкими.

Для этого потребуется министр обороны, который сосредоточит Департамент на ускорении внедрения новых технологий, и специальный Руководящий комитет по новым технологиям, чтобы стимулировать внедрение и согласовывать приоритеты между Министерством обороны и Разведывательным сообществом.

Секретарь должен руководить действиями в пяти областях:

1. Постройте техническую основу. Министерство обороны должно сделать фундаментальные инвестиции для поддержки технической инфраструктуры всего департамента для повсеместного развития и внедрения ИИ. Она сделала многообещающий первый шаг в 2020 году с выпуском Стратегии данных Министерства обороны. Однако Департаменту не хватает современной цифровой экосистемы, инструментов и сред для совместной работы, а также широкого доступа к общим ресурсам ИИ, необходимым для интеграции ИИ в рамках всей организации. Департаменту следует избегать переосмысления базовой инфраструктуры для каждой новой программы или потенциала, основанной на ИИ, и стремиться по возможности использовать проверенные решения Разведывательного сообщества (ИС) и взаимодействовать с ними. Более широкая платформа, которая могла бы использоваться во всем Департаменте, позволила бы более динамично развивать и использовать ИИ и более эффективно использовать скудный технический опыт.

Цифровая экосистема искусственного интеллекта.

Общие Интерфейсы ПОЛЬЗОВАТЕЛИ ПЛАТФОРМЕННЫЕ СРЕДЫ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДАННЫЕ ОБОРУДОВАНИЕ	Министр обороны должен руководить созданием цифровой экосистемы Министерства обороны. Секретарь должен потребовать, чтобы все новые совместные и сервисные программы соответствовали дизайну этой экосистемы и чтобы, где это возможно, существующие программы стали совместимыми с ней к 2025 году: • Архитектура данных, состоящая из защищённой федеративной системы распределённых хранилищ, связанных каталогом данных и соответствующими средствами контроля доступа, что облегчает поиск, доступ и перемещение нужных данных по всему мо. • Упакованные среды ИИ, которые позволяют гибко и итеративно развивать возможности ИИ, тестировать, внедрять и обновлять их в поддержку различных заинтересованных сторон.

• Рынок общих ресурсов ИИ, основанный на федеративных хранилищах данных, программного обеспечения и обученных моделей, а также предварительно согласованных вычислительных и хранилищных услугах пула проверенных облачных провайдеров.

• Укреплённая сеть и коммуникационная магистраль для обеспечения пропускной способности для поддержки транспорта и слияния данных, безопасной обработки, непрерывной разработки и внедрения приложений искусственного интеллекта и интеграции программных систем на всех уровнях.

• Общие интерфейсы, которые позволяют быстро интегрировать инвестиции, ориентированные на миссию.

«Воины не могут изменить то, как они сражаются, не изменив также и то, как они думают.»

Тренируйте и обучайте Бойцов.

Столбы				
Принятие решений на основе данных	Вычислительное мышление	Человеко-машинное объединение	Организационная трансформация	Культура создателя
Рекомендации				
Интегрируйте цифровые навыки и вычислительное мышление в обучение младших военных лидеров	Интеграция новых и прорывных технологий в профессиональное военное образование на уровне службы	Создание новых и прорывных технологий кодирования заготовок в МО		

2. Тренируйте и обучайте бойцов. Воюющие не могут изменить то, как они сражаются, не изменив также и то, как они думают. Большинство сотрудников службы используют мощные компьютеры только для создания презентаций PowerPoint, создания электронных таблиц или отправки электронной почты. Наши сотрудники должны развивать ключевые компетенции в создании, использовании и ответственном взаимодействии с

машинными системами, чтобы распознать потенциал ИИ для создания более быстрой и эффективной силы. В частности, они должны знать:

• Как использовать данные в процессе принятия решений, дополняя интуицию и опыт.

• Как использовать агенты обработки информации и как заставить компьютер выполнять вычисления и аналитику, которые не могут быть эффективно выполнены человеком.

• Как развиваться и процветать в культуре «создателя», которая поощряет непрерывный контакт и регулярные эксперименты с новыми инструментами.

• Как перейти к «модели партнёра по команде» для взаимодействия с автономными системами и ориентироваться в вопросах делегирования полномочий, наблюдаемости, предсказуемости, управляемости и доверия.

• Как привести организации в эру ИИ—в том числе когда и как интегрировать связанные с ИИ задачи в приоритетные миссии, выделять ресурсы для создания и обслуживания стека ИИ, контролировать новые системы и поддерживать карьеру технических экспертов.

Чтобы улучшить подготовку и образование в этом направлении, Министерство обороны должно:

• Определить членов службы, которые преуспели в вычислительном мышлении во время процесса присоединения;

• Инвестируйте в повышение квалификации своей рабочей силы с помощью самостоятельных образовательных курсов и стимулов к кодированию языка;

• Обучать младших руководителей курированию проблем, жизненному циклу ИИ, сбору и управлению данными, вероятностным рассуждениям и визуализации данных, а также принятию обоснованных решений на основе данных в рамках их требований к вводу в эксплуатацию и начальной подготовке;

• Интегрировать обучение новым и прорывным технологиям в курсы профессионального военного образования;

• Создание новых технологических кодированных заготовок и новой программы сертификации технологий, сопоставимой с совместной системой заготовок и квалификаций.

3. Ускорить внедрение существующих цифровых технологий. Министерство обороны в значительной степени полагалось на обходные пути для внедрения новых технологий, в то время как основные процессы приобретения остаются склеротическими.

Есть несколько ярких пятен, в том числе выпуск системы хвостовых закупок Департамента, контрактные ресурсы, и подходы, принятые некоторыми программами в Военно-воздушных силах.

Департамент должен масштабировать эту инновационную практику и предпринять дальнейшие шаги по согласованию подготовки кадров для приобретения, программных стимулов, бюджета и организационных структур для более эффективной поддержки предоставления возможностей с цифровыми возможностями.

Ряд инициатив Департамента по цифровым инновациям дал свои результаты, но они не скоординированы и недостаточно обеспечены ресурсами.

Сигнализация Минобороны о технологических приоритетах носит разовый характер и не подкрепляется послужным списком значительных инвестиций Минобороны в цифровые технологии с нетрадиционными поставщиками. В результате приложения ИИ для обеспечения национальной безопасности привлекают меньше частных инвестиций. Департамент должен сосредоточиться на четырёх действиях:

• Интеграция коммерческого ИИ для оптимизации основных бизнес-процессов. МО должно охватить проверенные коммерческие приложения ИИ и стимулировать их использование для создания экономии труда и затрат, ускорения административных действий и информирования процесса принятия решений. В качестве критического первого шага Министерство обороны должно уделять приоритетное внимание созданию корпоративных наборов данных по основным областям администрирования.

• Сетевые цифровые инновационные инициативы для масштабирования воздействия. Очаги инноваций снизу-вверх должны сочетаться с лидерством сверху вниз. Департаменту следует согласовать свои инновационные инициативы для осуществления скоординированной стратегии выхода на рынок коммерческих технологических решений. Заместитель министра обороны по научным исследованиям и инженерным разработкам, тесно сотрудничая с Заместителем министра обороны по закупкам и снабжению, военными службами и другими партнерами из штаб-квартиры, должен обеспечить стратегическое направление этих усилий.

• Расширить использование специализированных путей приобретения и контрактных подходов. Минобороны должно активизировать усилия по подготовке специалистов по закупкам по всему спектру доступных вариантов приобретения и заключения контрактов и стимулировать их использование для ИИ и цифровых технологий.

• Обновление бюджетных и надзорных процессов. Процесс распределения ресурсов Министерства обороны почти идентичен тому, что было введено в действие в 1961 году. Он несовместим с ИИ и другими цифровыми технологиями. Министерство обороны и Конгресс должны провести реформы, которые позволят развивать программное обеспечение и цифровые технологии, учитывая скорость, неопределённость, эксперименты и непрерывные обновления.

Доставка ИИ со скоростью и масштабом.

Комплексный и стратегический подход к технологиям, который согласовывает процесс, стимулы и организационную культуру Министерства обороны и инновационной базы национальной безопасности как конвейер для ресурсного обеспечения, приоритизации, приобретения и итерации возможностей, критически важных для поддержания конкурентного преимущества.

«На каждом уровне технологи, операторы и эксперты по предметной области должны функционировать как единые команды.»

4. Демократизировать развитие ИИ. Департамент должен содействовать развитию ИИ снизу-вверх. На каждом уровне технологи, операторы и эксперты по предметной области должны функционировать как единые команды. Это облегчило бы обратную связь с пользователями и повысило бы доверие к системам искусственного интеллекта. Минобороны должно:

• Назначить Объединённый центр искусственного интеллекта (JAIC) в качестве ускорителя искусственного интеллекта Департамента. JAIC не может определить каждое потенциальное использование ИИ в Отделе, но он может и должен служить центральным центром экспертизы ИИ. В рамках этой модели «ускорителя» JAIC будет координировать свои действия с соответствующими подразделениями по закупкам, технологиям и управлению для информирования о стратегии; разрабатывать приложения ИИ, которые решают общие задачи в командованиях боевых подразделений; и предоставлять ресурсы, позволяющие распределять разработку ИИ по всему департаменту и военным службам.

Во-первых, Министерство обороны сохраняет свой текущий уровень инвестиций в основной ИИ (~1,5 млрд долларов в год).

Во втором сценарии Министерство обороны увеличивает свои инвестиции в основной ИИ до $8 млрд в год.

Для повышения темпов внедрения ИИ требуется значительное увеличение основных расходов на ИИ.

Сотрудники NSCAI объединились с двумя внешними партнёрами для анализа исторических и планируемых инвестиций Министерства обороны в AI RDT&E. Исходными данными для анализа являются годовые расходы бюджета Министерства обороны на РДТ и Э (на 2015 – 2020 финансовый год) и годовые бюджетные запросы на РДТ и Э (на 2021-2025 финансовый год). Использованную методологию и уроки, извлечённые из этой работы, см. в

разделе Анализ инвестиций Министерства обороны в ИИ, NSCAI (в файле Комиссии).

Отказ от ответственности:

Мы считаем, что этот анализ даёт важную информацию об общих тенденциях в расходах на ИИ и решениях для лучшего будущего анализа, но предупреждаем, что проблемы с качеством исходных данных, подробно описанных в нашем отчёте, означают, что представленные оценки уровня расходов содержат значительные, трудно поддающиеся оценке пределы погрешности.

Программы с поддержкой ИИ разрабатывают (в случае программ RDT&E) и полевые (в случае программ закупок) гамму военных и бизнес-систем МО, включая Основные приложения ИИ для анализа, автоматизации, коммуникации, маневрирования, мониторинга, зондирования и многих других задач. Хотя расходы на ИИ обычно составляют небольшой процент от этих программ, производительность их системы может критически зависеть от включения основного ИИ.

Программы поддержки ИИ включают такие технологии, как облачные вычисления и передовая микроэлектроника, необходимые для поддержки развёртывания эффективных возможностей ИИ в масштабе.

• Создание интегрированных групп доставки ИИ в каждом боевом командовании. Эти команды имеют специфические оперативные потребности, которые обычно опережают централизованную разработку. Команды доставки ИИ должны быть встроены в каждое Боевое командование и способны поддерживать полный жизненный цикл разработки ИИ и полевых работ, включая науку о данных, проектирование, тестирование и производство, используя общие ресурсы через цифровую экосистему. Группы должны включать в себя компоненты передового развёртывания, которые будут действовать в качестве локального интерфейса с оперативными подразделениями.

5. Инвестируйте в возможности нового поколения. Руководители Министерства обороны ожидают, что оборонные бюджеты на ближайшие годы останутся неизменными или сократятся.29 Несмотря на потенциальное

бюджетное давление, Министерство обороны должно продолжать ускорять свои программы модернизации, уделяя приоритетное внимание новым и разрушительным технологиям, таким как ИИ.

• Финансировать исследования и разработки в области ИИ. Департамент должен взять на себя обязательство тратить не менее 3,4% своего бюджета на науку и технику и ежегодно выделять не менее 8 миллиардов долларов на исследования и разработки в области ИИ.31 Дополнительные ресурсы должны быть сосредоточены на организациях, обладающих значительным опытом в области искусственного интеллекта, таких как Агентство перспективных исследовательских проектов обороны (DARPA), Управление военно-морских исследований (ONR), Управление научных исследований ВВС (AFOSR), Армейское исследовательское управление (ARO) и служебные лаборатории.

«Чтобы сделать ИИ повсеместным во всех своих бизнес-процессах и военных системах, Минобороны должно пойти на жёсткие бюджетные компромиссы и расставить приоритеты модернизации.»

• Вывод на пенсию устаревших систем, плохо оснащённых для участия в боевых действиях с использованием ИИ. Чтобы сделать ИИ повсеместным во всех своих бизнес-процессах и военных системах, Минобороны должно пойти на жёсткие бюджетные компромиссы и расставить приоритеты модернизации. Министерство обороны должно придерживаться сбалансированного подхода к обновлению существующих систем с использованием передовых технологий, чтобы выиграть время для инвестиций в долгосрочные ставки.

Кроме того, чтобы избежать предвзятости в пользу защиты статус-кво, Минобороны должно потребовать оценки альтернатив ИИ до финансирования Крупных программ оборонных закупок (MDAP).

• Подготовить технологическое приложение к Стратегии национальной обороны. Чтобы увязать стратегию инвестиций в технологии Министерства обороны с будущими оперативными потребностями, приложение должно включать дорожные карты для проектирования, разработки, внедрения и

поддержания критических технологий, необходимых для решения оперативных задач, определённых в стратегии.

Примечания

1. Генерал Джозеф Данфорд, тогдашний председатель Объединённого комитета начальников штабов, свидетельствовал в 2017 году, что «конкурентное преимущество американских военных перед потенциальными противниками размывается […] Я оцениваю, что в течение пяти лет мы потеряем способность проецировать силу; основу того, как мы защищаем родину, продвигаем США и выполнять наши союзнические обязательства.» Заявление о позиции генерала Джозефа Данфорда, Председателя Объединённого комитета начальников штабов перед Сенатским комитетом по вооружённым силам, слушание бюджета Сената по вооружённым силам на 2 (13 июня 2017 года), https://www.armed-services.senate.gov/imo/media/doc/Dunford_06-13-17.pdf.

2. Big Data at War: Special Operations Forces, Project Maven, and Twenty-First-Century Warfare, Modern War Institute (25 августа 2020 г.), https://mwi.usma.edu/big-data-at-war-special-operationsforces-project-maven-and-twenty-first-century-warfare/; Шерил Пеллерин, Проект Maven по развертыванию компьютерных алгоритмов в зоне боевых действий к концу года, Министерство обороны (21 июля 2017 года), https://www.defense.gov/Explore/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-byyears-end/. Проект Maven теперь включает в себя обнаружение, классификацию и отслеживание объектов в видеоизображениях полного движения (например, человека, транспортного средства и оружия) и другие алгоритмы искусственного интеллекта для текстовых проектов. PE 0305245D8Z: Разведывательные возможности и инновации, Канцелярия министра обороны (февраль 2019 года), https://www.dacis.com/budget/budget_pdf/FY20/RDTE/D/0305245D8Z_187.pdf.

3. Например, армейские учения «Конвергенция проекта» в сентябре 2020 года продемонстрировали использование ИИ на нескольких этапах процесса

целеуказания. Джен Джадсон и Натан Страут, В Проекте Конвергенция армия США Пережила Успех и Неудачу—и Она Счастлива И Тем, и Другим, Defense News (12 октября 2020 года), https://www.defensenews.com/digital-show-dailies/ausa/2020/10/12/at-project-convergencethe-us-army-experienced-success-and-failure-and-its-happy-about-both/. Военно—воздушные силы провели аналогичные учения, прежде всего в рамках своих усилий, связанных с Передовой системой боевого управления-технической инфраструктурой, которая будет поддерживать Совместную концепцию управления и управления всеми областями МО. Тереза Хитченс, Демонстрация ABMS Доказывает, Что AI Chops For C2, Breaking Defense (3 Сентября 2020 года), https://breakingdefense.com/2020/09/abms-demo-proves-ai-chops-for-c2/.

4. Это включает в себя традиционный процесс, посредством которого концепции функционирования взаимодействуют с развитием технологий. В главе 3 настоящего доклада предлагаются рекомендации по адаптации этого подхода и обеспечению того, чтобы технологические достижения в той же мере информировали концепции, в какой концепции стимулировали развитие технологий.

5. Как заметил один наблюдатель: «Хотя инвестиционные счета Министерства обороны существенно выросли за последние три года, этот рост был в значительной степени сосредоточен на покупке систем с существующих производственных линий и создании прототипов военных систем.» Показания Эндрю Хантера, директора Группы оборонно-промышленных инициатив CSIS, перед Комитетом по вооруженным силам Палаты представителей США, слушая о роли Министерства обороны в конкуренции с Китаем в 6 (янв. 15, 2020), https://armedservices.house.gov/_cache/files/5/8/5818cc1f-b86f-4dca-8aee-10ca788e6f43/9F4A03ABF1DEAB747AF2D1302087A426.20200115-hasc-andrew-hunter-statement-vfinal.pdf.

6. Стратегия национальной обороны подчеркивает важность инновационной базы национальной безопасности в поддержании технологического преимущества Департамента. Краткое изложение Стратегии национальной

обороны на 2018 год, Министерство обороны США на 3 (2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf. Центр стратегических и международных исследований предлагает полезное определение этого термина, отмечая, что «[Инновационная база национальной безопасности] представляет собой значительное расширение сферы охвата [...] по сравнению с традиционной концепцией оборонно-промышленной базы» и включает в себя технологические фирмы из инновационных центров, таких как Силиконовая долина, Бостон и Остин. См. Эндрю Хантер, Стратегический подход к оборонным инвестициям, CSIS (26 марта 2018 г.), https://www.csis.org/analysis/strategic-approach-defense-investment.

7. Крупнейшие шесть основных оборонных поставщиков (Lockheed Martin, Boeing, Northrop Grumman, Raytheon, General Dynamics и BAE Systems) [...] представляли 32 процента всех основных обязательств Министерства обороны в 2019 году.» 2020 финансовый год: Промышленный потенциал, Министерство обороны США на уровне 40 (23 декабря 2020 года), https://www.businessdefense.gov/Portals/51/USA002573-20%20ICR_2020_Web.pdf?ver=o3D76uGwxcg0n0Yxvd5k-Q%3d%3d.

8. Стратегия закладывает основу для того, чтобы Департамент рассматривал данные как стратегический актив, и детализирует цели, направленные на то, чтобы сделать данные Министерства обороны видимыми, доступными, понятными, связанными, заслуживающими доверия, совместимыми и безопасными. Резюме: DoD Data Strategy, Министерство обороны США (30 сентября 2020 г.), https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF.

9. В последние годы Департамент предпринял многообещающие начальные шаги по созданию конструкций управляемых сервисов для платформ, облачной инфраструктуры и разработки программного обеспечения. Например, предложения BBC CloudOne и PlatformOne (https://software.af.mil/dsop/services/); Чёрная жемчужина военно-морского флота (https://blackpearl.us/); и Армейское хранилище кодирования и среда

преобразования (CReATE). Кроме того, Управление министра обороны создало платформу управления данными ADVANTAGE с целью создания ее в качестве единственного авторитетного источника для аудита и анализа бизнес-данных. См. Письменное заявление заместителя министра обороны Дэвида Л. Норквиста перед Подкомитетом Комитета по вооружённым силам Сената США по вопросам готовности в 6 часов (20 ноября 2019 года). https://www.armed-services.senate.gov/imo/media/doc/Norquist_11-20-19.pdf.

10. Компоненты этой платформы разрабатываются в результате Совместной инициативы Объединённого центра искусственного интеллекта (JAIC) в частности, рынка общих ресурсов ИИ, включая данные, алгоритмы и обученные модели ИИ.

11. Использование общей технической инфраструктуры значительно повысит способность Министерства обороны обеспечивать оперативную совместимость и повысить эффективность объединённых сил. Однако важно отметить, что даже без такой критической технической инфраструктуры Департамент предпринимает важные политические шаги для обеспечения интероперабельности и готовности ИИ к программам, предназначенным для удовлетворения совместных потребностей в потенциале. См. Aaron Mehta, Hyten to Issue New Joint Requirements on Handling Data, Defense News (23 сентября 2020 г.), https://www.defensenews.com/pentagon/2020/09/23/hyten-to-issue-new-joint-requirements-onhandling-data/. В главе 3 настоящего доклада излагаются дополнительные рекомендации по достижению состояния готовности военного ИИ к 2025 году.

12. Защищённый доступ к наборам данных, а также к другим общим ресурсам должен управляться с помощью аутентификации на основе пользователей и ролей, облегчаемой сквозной инфраструктурой идентиикации, учетных данных и управления доступом.

13. Это зависит от реализации новой информационной стратегии Министерства обороны. Резюме: DoD Data Strategy, Министерство обороны США (30

сентября 2020 г.), https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF.

14. Это платформенные среды с готовыми рабочими процессами, которые могут быть адаптированы и запущены в зависимости от типа пользователя (например, исследователь, отраслевой партнёр, оператор) и варианта использования (например, разработка, TEVV [test, evaluation, validation, verification], fielding).

15. Другими словами, жизненный цикл приложения DevSecOps. «DevSecOps улучшает время выполнения и частоту результатов доставки за счет улучшения инженерных практик, способствуя более сплочённому сотрудничеству между командами разработки, безопасности и операций, поскольку они работают в направлении непрерывной интеграции и доставки.» Понимание различий между Agile и DevSecOps. С точки зрения бизнеса, GSA (последний доступ 1 января 2021 года), https://tech.gsa.gov/guides/understanding_differences_agile_devsecops/.

16. Заинтересованные стороны могут включать в себя встроенные команды разработчиков, работающие на тактическом фронте; партнёров из частного сектора, предоставляющих предварительно подготовленные модели; академических исследователей, работающих над открытыми актуальными проблемами; правительственных исследователей науки и техники (S&T), работающих в рамках сервисной лаборатории; или международных партнеров, совместно разрабатывающих совместимые возможности ИИ.

17. Общие ресурсы ИИ должны управляться с постоянной авторизацией для работы фреймворков (ATO) и с обязательной взаимностью ATO по умолчанию во всем Департаменте.

18. Аналогично или полагаясь на платформу доставки и функции Git (https://git-scm.com), GitHub (https://github.com), и GitLab (https://about.gitlab.com).

19. Адаптивная система закупок и Контрактный конус управления закупок Пентагона знаменуют собой важные шаги Департамента

по содействию использованию альтернативных органов власти для закупок и контрактов. К ним относятся, например, другие органы управления транзакциями, приобретения среднего уровня, быстрое прототипирование и быстрое внедрение, а также специализированные пути приобретения программного обеспечения.

20. Например, Усовершенствованная система боевого управления ВВС (ПРО), которая представляет собой управляющие системы, предназначенные для поддержки новой концепции Совместного Общесоциального командования и управления в качестве портфеля и в значительной степени основанные на экспериментах для стимулирования инноваций и итеративного подхода к требованиям. Примечательно, что Законопроект об ассигнованиях Министерства обороны на 2021 финансовый год выражает озабоченность различными аспектами подхода ВВС, включая «отсутствие твёрдых требований, стратегии приобретения или сметы расходов» и системы системной интеграции. См. H. Rept. 116-453, в 294-295 (16 июля 2020 года), https://www.congress.gov/116/crpt/hrpt453/CRPT-116hrpt453.pdf.

21. Термин «цифровые инновационные инициативы» используется здесь для описания различных структур в Офисе министра обороны и военных службах, таких как Подразделение оборонных инноваций (DIU), AFWERX, NavalX и Лаборатория армейских приложений (AAL), которые сосредоточены на преодолении разрыва с коммерческим технологическим сектором, особенно стартапами и нетрадиционными поставщиками, и ускорении доставки лучших в своём роде технологических решений.

22. Подразделение оборонных инноваций (DIU) в настоящее время реализует ряд проектов ИИ по оптимизации бизнес-процессов в Минобороны, начиная от использования роботизированной автоматизации процессов ИИ для снижения затрат на рабочую силу для Армейского контролера и заканчивая повышением готовности ВВС с помощью управляемого ИИ прогнозного обслуживания и использованием построенных ИИ графиков знаний для быстрого выявления рисков цепочки поставок для

Оборонного разведывательного управления. См. JAIC Partners with DIU on AI/мл Models to Resolve Complex Financial Errors, JAIC (Oct. 1, 2020), https://www.ai.mil/blog_10_01_20-jaic_partners_with_diu_on_aiml_models_to_resolve_complex_finanical_errors.html; Награды Министерства обороны США C3.ai Контрактная машина стоимостью 95 млн долларов для повышения готовности воздушных Судов с использованием искусственного интеллекта, Business Wire (15 января 2020 года), https://www.businesswire.com/news/home/20200115005413/en/US-Defense-Department-Awards-C3 аи-95M-Контракт-Транспортное средство-для-улучшения-готовности-самолёта-Использование-ИИ; Ускорять.ИИ Ускоряет рост и внедрение продукции с контрактом на оборонное инновационное подразделение, Accrete.ai (23 апреля 2020 года), https://blog.accrete.ai/newsroom/accrete.ai-wins-million-dollar-contract-with-the-defense-innovation-unit.

23. Например, DIU использует несколько путей приобретения и контрактных стратегий, которые могут помочь улучшить как принятие, так и оперативную актуальность решений ИИ, а также расширить инновационную базу национальной безопасности. DIU впервые открыла Коммерческие решения с Армейским контрактным командованием–Нью-Джерси, которое использует раздел 2371b раздела 10 Usc Other Transaction authority для создания «быстрого, гибкого и совместного» контрактного транспортного средства для прототипирования возможностей Департамента. DIU также использовала раздел 2374a раздела 10 U. S. C. Prize Challenge Authority для продвижения различных приоритетов, связанных с ИИ, для Министерства обороны и более широкого сообщества исследователей ИИ.

24. Описанная выше цифровая инфраструктура в масштабах всего департамента имеет решающее значение для реализации этого подхода, но для максимизации его полезности также необходимы структурные изменения.

25. Есть заметные примеры пар военных истребителей-технологов в МО, такие как заводы программного обеспечения ВВС и передовые группы

тактических данных, используемые Командованием специальных операций и армейским командованием будущего. Они обнаружили, что партнёрство технологов (например, специалистов по обработке данных) с операторами или аналитиками на тактическом фронте: 1) значительно сокращает время, обычно необходимое подрядчику для понимания поставленной проблемы и развёртывания решения.; 2) стимулирует итеративные методы разработки и быстрое внедрение минимально жизнеспособных продуктов, которые дают решения с более высокой отдачей в ускоренные сроки; и 3) генерирует повышенный интерес к данным и технологиям искусственного интеллекта как к решающим инструментам выполнения задач. ВОЕННО - МОРСКИЕ бои (ноябрь 2020 года). Чтобы обеспечить американским силам сохранение превосходства в долгосрочной перспективе, Минобороны должно масштабировать это ориентированное на пользователя развитие.

26. Важные подразделения для координации с JAIC включают, но не ограничиваются ими, USD(R&E), USD Acquisition & Sustainment (USD(A&S)), Director Operational Test & Evaluation (DOT&E), а также DoD Chief Information Officer (CIO) и Chief Data Officer (CDO). В рамках USD(R&E) DIU является ключевым активатором JUICE, который придерживается проектного подхода, переводя коммерческие прототипы для конкретных применений. В настоящее время «ДЖЕНИС» обслуживает Боевые командования через свои Компонентные инициативы миссии (CMIs), включая Инициативу Миссии по совместным боевым операциям. См. Mission Initiatives, JAIC (последний доступ 28 декабря 2020 года), https://www.ai.mil/mi_joint_warfighting_operations.html.

27. Такие приложения могут быть разработаны другими боевыми командованиями, фабриками служебного программного обеспечения или СОКОМ и доступны через рекомендуемую цифровую экосистему. Каждая боевая команда должна обеспечить, чтобы команды доставки ИИ были укомплектованы соответствующими талантами для управления полным жизненным циклом решений ИИ, в том числе в таких дисциплинах, как наука о

данных, тестирование ИИ и обучение моделям, разработка программного обеспечения, управление продуктами и разработка полного стека.

28. Например, как Командование армейских фьючерсов (AFC), так и Командование армейских специальных операций (USASOC) используют модель, известную как «тактические группы данных».» Эта модель приносит опыт ИИ/мл в поле в виде команд из трех - шести человек для создания ИИ-решений для оперативных задач в реальном времени. Выполняемые малым бизнесом, Strive works, по контракту с АФК и USASOC, они в настоящее время поддерживают усилия в Зонах ответственности Центрального командования и Индо-Тихоокеанского командования.

Глава 2 - Концевые примечания

29. Джим Гарамон, Председатель Комитета по будущим оборонным бюджетам Министерства обороны США (3 декабря 2020 года), https://www.defense.gov/Explore/News/Article/Article/2433856/chairman-discusses-futuredefense-budgets/.

30. Краткое изложение Стратегии национальной обороны на 2018 год, Министерство обороны США на 6 (2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

31. Совет по оборонной науке в прошлом предлагал уровень в 3,4%, чтобы отразить типичную практику в частном секторе. Министерство оборонных исследований, разработок, испытаний и оценки (RDT&E): Структура ассигнований, Исследовательская служба Конгресса в 12 (7 октября 2020 года), https://fas.org/sgp/crs/natsec/R44711.pdf.

32. В докладе Целевой группы «Будущее обороны «также говорилось, что» политики, промышленность и Пентагон должны работать вместе, чтобы определить компромиссы в рамках оборонного аппарата, чтобы включить унаследованные системы и операции, которые позволят инвестировать в технологии и оперативные концепции для решения будущих проблем.» Доклад Целевой группы по будущему обороны 2020 года, Комитет по вооруженным

силам Палаты представителей в 18 (23 сентября 2020 года), https://armedservices.house.gov/_cache/files/2/6/26129500-d208-47ba-a9f7-25a8f82828b0/424EB2008281A3C79BA8C7EA71890AE9.future-of-defense-task-forcereport.pdf.

33. Это должно использовать wargaming, эксперименты и живую виртуальную конструктивную среду везде, где это возможно, и должно предусматривать взаимодействие с цифровой экосистемой. Этот момент перекликается с будущим Defense Task Force, которая рекомендовала, чтобы каждая Крупная программа оборонных закупок (MDAP) должна была «оценить по крайней мере один ИИ или автономную альтернативу до начала финансирования».

ИИ и война

ИИ готов к 2025 году

Лидерство сверху вниз. Инновационные Концепции. Цели эффективности ИИ-Готовности. Передовые технологии и НИОКР. Союзники и партнёры с поддержкой ИИ.

Даже при наличии правильных технологических основ искусственного интеллекта (ИИ) американские военные все равно окажутся в невыгодном положении на поле боя, если им не удастся принять правильные концепции и операции для интеграции технологий ИИ.

На протяжении всей истории лучшие адепты и интеграторы, а не лучшие технологи, пожинали военные награды новых технологий. Министерство обороны (МО) не должно быть свидетелем революции ИИ в военном деле, но должно обеспечить её с руководством сверху, новыми операционными концепциями, неустанными экспериментами и системой, которая вознаграждает ловкость и риск.

Благодаря ИИ возникает новая парадигма ведения боевых действий. Наши конкуренты делают значительные инвестиции, чтобы воспользоваться этим преимуществом. Эта идея была названа «алгоритмической» или «мозаичной» войной; китайские теоретики назвали её «интеллигентизированной» войной. Все эти термины по-разному отражают то, как в новой эре конфликта будет доминировать ИИ и противопоставлять алгоритмы алгоритмам.

Преимущество будет определяться количеством и качеством военных данных, алгоритмами, которые они разрабатывают, сетями с поддержкой ИИ, которые они подключают, управляемым оружием, которое они используют, и операционными концепциями с поддержкой ИИ, которые они используют для создания новых способов ведения войны.

Сегодняшнее Министерство обороны США пытается выполнить поворот ИИ, но без срочности. Несмотря на очаги творческих реформ и нескольких дальновидных лидеров, МО остаётся запертым в менталитете индустриального века, в котором конфликт великих держав рассматривается как соревнование массовых сил и монолитных платформ и систем.

Растущее повсеместное распространение ИИ в коммерческой сфере и скорость цифровой трансформации подчёркивают риск недостаточно быстрого поворота.

Департамент должен действовать сейчас, чтобы интегрировать ИИ в критические функции, существующие системы, учения и военные игры, чтобы стать уже силой к 2025 году.

Одновременно Минобороны должно разработать более креативные концепции ведения боевых действий, которые сочетаются с инвестициями в будущие технологии с поддержкой искусственного интеллекта, чтобы постоянно опережать потенциальных противников. Если наши силы не будут оснащены системами с поддержкой искусственного интеллекта, управляемыми новыми концепциями, превосходящими концепции их противников, они будут превосходить и парализованы сложностью боя.

Это уже сделано к 2025 году:

Warfighters обеспечили базовую цифровую грамотность и доступ к цифровой инфраструктуре и программному обеспечению, необходимым для повсеместной интеграции ИИ в обучение, учения и операции.

«Департамент должен действовать сейчас, чтобы интегрировать ИИ в критические функции, существующие системы, учения и военные игры, чтобы стать готовыми к ИИ силами к 2025 году».

Чтобы конкурировать, сдерживать и, при необходимости, бороться и побеждать в будущих конфликтах, требуется полная корректировка оперативных концепций, технологий, организационных структур и того, как мы интегрируем союзников и партнёров в операции. Это также потребует оценки рисков как преимуществ, так и недостатков широко распространённой

интеграции возможностей ИИ, включая будущие автономные системы вооружения.

Наконец, для этого потребуется готовность участвовать в двустороннем и многостороннем диалоге с нашими союзниками и партнёрами, чтобы побудить их сделать аналогичные поворотные точки ИИ для обеспечения будущей оперативной совместимости.

Война с использованием ИИ не будет зависеть от одного нового оружия, технологии или оперативной концепции; скорее, она будет сосредоточена на применении и интеграции технологий с использованием ИИ во все аспекты боевых действий. ИИ изменит способ ведения войны во всех областях от подводного до космического пространства, а также в киберпространстве и вдоль электромагнитного спектра. Это повлияет на принятие стратегических решений, оперативные концепции и планирование, тактические манёвры на местах и поддержку бэк-офиса.

В этом новом виде войны традиционные границы поля боя будут расширены за счёт микро-маркетинга с поддержкой ИИ, дезинформации и кибероперациий, как описано в главе 1 настоящего доклада. ИИ изменит многие атрибуты войны, такие как её скорость, темп и масштаб; отношения военнослужащих с машинами; настойчивость, с которой можно наблюдать за полем боя; различение и точность, с которыми можно атаковать цели. Скорость и точность в развитии знаний, действиях и реакциях по мере развития конфликта будут иметь большое значение.

«Война с использованием искусственного интеллекта не будет зависеть от одного нового оружия, технологии или операционной концепции; скорее, она будет сосредоточена на применении и интеграции технологий AIenabled в каждый аспект боевых действий.»

Инвестиции Министерства обороны в ИИ хорошо распределены по различным областям ведения боевых действий (сухопутные, военно-морские, воздушные, космические, кибернетические, электромагнитные, информационные), причём более 25% инвестиций приходится на

многодоменные приложения ИИ, что свидетельствует о потенциале ИИ для интеграции многодоменных операций.

Инвестиции в приложения ИИ для космических операций выросли более чем в четыре раза с 2019 по 2025 финансовый год, с $500 млн до $2,2 млрд, увеличившись с 3% до почти 9% инвестиций с поддержкой ИИ.

Примечание:

Уровни расходов, представленные на рисунке, представляют собой оценки, основанные на анализе бюджетных документов Министерства обороны RDT&E на 2021-2025 финансовый год. См. Анализ инвестиций DoD RDT&E в AI, NSCAI (по окончательному согласованию с Комиссией).

Из-за присущих исходным данным проблем с качеством представленные оценки содержат значительные, трудно поддающиеся оценке пределы погрешности.

ИИ сделает процесс поиска и поражения целей военного значения более быстрым и эффективным. Это также повысит точность идентификации целей и минимизирует сопутствующий ущерб.

В настоящее время этот процесс обычно включает в себя последовательную передачу данных от датчика через ряд людей на платформу, которая может стрелять по цели. ИИ поможет автоматизировать некоторые промежуточные этапы процесса принятия решений. ИИ также создаст возможности для более продвинутых процессов, которые будут работать более сродни сети, объединяя множество датчиков и платформ для управления сложными потоками данных и передачи полезной информации операторам-людям и машинам во всех областях.4

Во время войны многие военные применения ИИ будут дополнять, а не вытеснять роль людей. Инструменты ИИ улучшат то, как сотрудники службы воспринимают, понимают, принимают решения, адаптируются и действуют в ходе выполнения своих задач. Однако новые концепции военных операций также должны будут учитывать меняющиеся способы, с помощью которых

люди смогут делегировать все более сложные задачи системам с поддержкой ИИ.

В ближайшей перспективе это будет осуществляться с помощью военного принципа «командования миссией», который подчёркивает децентрализованное исполнение и дисциплинированную инициативу подчинённых, которые следуют намерениям командира.

Этот ориентированный на человека подход к борьбе должен оставаться стандартом в обозримом будущем. Но по мере того, как ИИ продолжает продвигаться в когнитивную и нейроморфную область, а человеко-машинное объединение становится все более сложным, военным придётся разрабатывать более творческие концепции и организационные конструкции, которые в полной мере используют технологии ИИ, не отказываясь от принципов, лежащих в основе командования миссией.

Инновации приведут к будущим возможностям, которые в настоящее время непознаваемы и станут яснее только со временем.

Вместе Сильнее.

Если Соединённые Штаты хотят бороться с ИИ, им понадобятся союзники и партнёры с военными и разведывательными службами, поддерживающими ИИ. Неравномерное внедрение ИИ будет угрожать интероперабельности, политической сплочённости и устойчивости альянсов США.5 По мере углубления и расширения обычных оборонных механизмов по всему миру, особенно в Европе и Индопацифике. Соединённые Штаты должны включать ИИ и новые технологии в скоординированную оборонную и разведывательную деятельность. С учётом двойного назначения многих программных средств МО потребуется большая гибкость в работе с гражданскими учреждениями, компаниями и исследовательскими институтами в странах-партнёрах.

Рекомендация

Содействовать интероперабельности ИИ и внедрению критически важных новых технологий среди союзников и партнёров, включая «Пять глаз»,

Организацию Североатлантического договора (НАТО) и страны Индо-Тихоокеанского региона. Это должно включать в себя:

• Усиление существующих усилий в области обороны и разведки, связанных с ИИ Пять глаз.

• Поддержка усилий НАТО по ускорению соглашений об архитектуре и стандартах, развитию технического опыта союзников и поиску вариантов использования коалиционного ИИ для учений и военных игр.

• Содействие Международному партнёрству ИИ в области обороны Объединённого центра искусственного интеллекта (JAIC) как важнейшему средству дальнейшего сотрудничества в области обороны и безопасности ИИ.6

• Создание Атлантико-Тихоокеанского партнёрства в области технологий безопасности для улучшения военного и разведывательного потенциала и взаимодействия между европейскими и Индо-Тихоокеанскими союзниками и партнёрами.

«Неравномерное внедрение ИИ будет угрожать военной интероперабельности, а также политической сплочённости и устойчивости альянса США. «

Достичь состояния готовности военного ИИ к 2025 году.

Чтобы достичь этой цели, МО США должно:

Проведите организационную реформу через руководство сверху вниз. Старшие гражданские и военные чиновники должны чётко определять приоритеты и направления, наделять подчинённых полномочиями и принимать повышенную неопределённость и риск при освоении новых технологий.

В частности, МО должно:

• Создать Руководящий комитет высокого уровня по новым технологиям под председательством заместителя министра обороны, заместителя председателя Объединённого комитета начальников штабов и главного заместителя директора национальной разведывании;

• Обеспечить, чтобы директор JAIC оставался трёхзвёздочным генералом или флаг-офицером со значительным оперативным опытом, который подчиняется непосредственно министру обороны или заместителю министра обороны;

• Назначить заместителя министра обороны по научно-техническим исследованиям сопредседателем и главным научным советником Объединённого совета по надзору за требованиями;

• Назначьте оперативного адвоката ИИ в штат каждого боевого командования. Этот сотрудник будет выполнять ту же роль, что и Штатный судья-адвокат. Он или она будет экспертом в системах ИИ, будет консультировать командира и персонал о возможностях и ограничениях систем ИИ и определять, когда системы с поддержкой ИИ используются ненадлежащим образом.

Разработка инновационных оперативных концепций, интегрирующих новые боевые возможности с новыми технологиями. Эти концепции должны быть направлены на обеспечение бесперебойной оперативной совместимости между военными службами и оперативными областями. Разработчики концепции должны работать в тесном сотрудничестве с технологами, чтобы сформулировать, как военные могут наиболее эффективно сражаться в будущих сценариях, и они должны предположить, что возможности ИИ будут повсеместно использоваться на будущих полях сражений.

Эти концепции также могут стимулировать будущие инвестиции.

К концу 2021 года установите цели эффективности ИИ и цифровой готовности. Для достижения более существенной интеграции ИИ в рамках Мо заместитель министра обороны должен:

• Направлять компоненты МО для оценки военного ИИ и цифровой готовности через существующие форумы и процессы управления готовностью. Руководящий комитет по новым технологиям, возглавляемый тремя председателями, должен тесно сотрудничать с заместителем министра обороны по кадрам и готовности и Объединённым штабом для обеспечения того, чтобы

выявленные критерии готовности ИИ были включены в стратегии отчётности о готовности военных служб и обеспечения ресурсами.

• Поручить военным службам ускорить рассмотрение конкретных пробелов в навыках ИИ для информирования о стратегиях набора персонала и управления талантами.

• Поручить военным службам в координации с Заместителем министра обороны по закупкам и обеспечению, Объединённым штабом, Агентством оборонного снабжения и ЯИК уделять приоритетное внимание интеграции ИИ в системы материально-технического обеспечения и обеспечения там, где это возможно.

• Интегрируйте ИИ в основные военные игры и учения, чтобы продвигать полевые подходы к освоению технологий. Операторы нуждаются в постоянном взаимодействии с возможностями ИИ на ранних этапах цикла разработки, чтобы генерировать критическую обратную связь о том, как они функционируют и как они влияют на миссию. Широкое экспериментирование будет способствовать как разработке концепции, так и повышению эффективности технологии.

• Стимулировать эксперименты с приложениями, поддерживающими искусственный интеллект, через Стимулирующий фонд Warfighting Lab, который мог бы контролироваться предлагаемым Руководящим комитетом под председательством трёх председателей.

Определите совместную сетевую архитектуру боевых действий к концу 2021 года. Ключевой целью этой совместной сети боевых действий должна стать безопасная сеть систем с открытыми стандартами, поддерживающая интеграцию приложений искусственного интеллекта на оперативном уровне и в различных областях. Он должен быть доступен всем военным службам и охватывать несколько элементов, включая сети командования и управления; передачу, хранение и безопасную обработку данных; и интеграцию систем вооружения. Техническая инфраструктура сети должна поддерживаться лучшими практиками в области цифровой инженерии.14 Она также должна

быть совместима с цифровой экосистемой, описанной в главе 2 настоящего доклада.

Инвестируйте в приоритетные области исследований и разработок в области ИИ, которые могли бы поддержать будущий военный потенциал, включая следующие:

Примечания

1. О военном усыновлении см., например, Michael C. Horowitz, The Diffusion of Military Power: Causes and Consequences for International Politics, Princeton University Press (2010).

2. Центральная концепция Mosaic warfare Agency of Defense Advanced Research Projects Agency (DARPA) построена вокруг «адаптивности для американских сил и сложности или неопределенности для противника за счет быстрого состава и перекомпоновки более дезагрегированных вооруженных сил США с использованием человеческого командования и управления машинами».» Брайан Кларк и др., Mosaic Warfare: Использование искусственного интеллекта и автономных систем для реализации операций, ориентированных на принятие решений, CSBA at vi (Feb. 11, 2020), https://csbaonline.org/research/publications/mosaic-warfare-exploiting-artificial-intelligence-andautonomous-systems-to-implement-decision-centric-operations/publication/1.

3. Народно-освободительная армия разработала концепцию ведения боевых действий для того, что она называет «интеллектуальными операциями» с ИИ в своей основе. В рамках этой конструкции Китай теоретизирует, что в будущем конфликте центральное соперничество будет происходить между противоборствующими боевыми сетями, а не традиционными оружейными платформами, и что информационное преимущество и алгоритмическое превосходство будут определяющими факторами победы. См. Elsa Kania, Chinese Military Innovation in Artificial Intelligence, CLASS at 1 (7 июня 2019), https://www.cnas.org/publications/congressional-testimony/chinese-military-

innovation-in-artificial-intelligence (показания перед американо-китайской комиссией по обзору экономики и безопасности).

4. См. Раздел Создание междоменных сетей уничтожения в режиме реального времени, DARPA (18 сентября 2020 г.), https://www.darpa.mil/news-events/2020-09-18a. См. также AI Fusion: Enabling Distributed Artificial Intelligence to Enhance Multi-Domain Operations & Real-Time Situational Awareness, Carnegie Mellon University (2020), http://www.cs.cmu.edu/~ai-fusion/overview.

5. О проблемах военной интероперабельности, связанных с ИИ, см. Эрик Лин-Гринберг, Союзники и искусственный интеллект: препятствия для операций и принятия решений, Texas National Security Review (Весна 2020), https://tnsr.org/2020/03/allies-and-artificial-intelligence-obstacles-to-operations-and-decisionmaking/.

6. Партнёрство ИИ в интересах обороны, начатое в сентябре 2020 года, включает Соединённые Штаты и 12 стран-партнёров: Австралию, Канаду, Данию, Эстонию, Финляндию, Францию, Израиль, Японию, Норвегию, Южную Корею, Швецию и Великобританию. Она стремится «обеспечить основанное на ценностях глобальное лидерство» в принятии ИИ в контексте обороны и безопасности и объединить «страны-единомышленники для содействия ответственному использованию ИИ, продвижения общих интересов и передовой практики внедрения этики ИИ, создания рамок для содействия сотрудничеству и координации стратегических сообщений по политике ИИ.» Совместное заявление, AI Partnership for Defense (15-16 сентября 2020 г.), https://www.ai.mil/docs/AI_PfD_Joint_Statement_09_16_20.pdf. Партнерство провело свой второй официальный диалог в январе 2021 года. DoD Joint AI Center Облегчает Второй Международный диалог по ИИ для обороны, JAC (27 января 2021 года), https://www. ai.mil/news_01_27_21-dod_joint_ai_center_facilitates_second_international_ai_dialogue_for_defense.html.

7. Комиссия признает раздел 236 Закона о разрешении национальной обороны на 2021 финансовый год, который разрешает министру обороны создать руководящий комитет по новым технологиям и угрозам национальной

безопасности в составе заместителя министра обороны, заместителя председателя Объединённого комитета начальников штабов, Заместителя министра обороны по разведке и безопасности, Заместителя министра обороны по исследованиям и инженерным разработкам, Заместителя министра обороны по персоналу и готовности, Заместителя министра обороны по закупкам и обеспечению, Главного сотрудника по информации., и таких других чиновников Министерства обороны, как секретарь, считает подходящими. Однако структура, описанная в разделе 236, не включает в себя руководство со стороны Разведывательного сообщества и, таким образом, не будет управлять намеченными действиями. См. Pub. L. 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021).

8. В частности, в Стратегии национальной обороны подчёркивается необходимость «разработки инновационных оперативных концепций» и «воспитания культуры экспериментирования и расчётливого принятия рисков».» Более тесная координация между разработчиками концепций и технологами создаст более динамичный цикл развития и интеграции технологий. Краткое изложение Стратегии национальной обороны на 2018 год, Министерство обороны США на 7 (2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-DefenseStrategy-Summary.pdf.

9. «Готовность» является ключевым показателем военной эффективности и остаётся в центре бюджетных, политических и надзорных дебатов по вопросам готовности к обороне. В этом контексте Минобороны должно установить ключевые цели эффективности ИИ и цифровой готовности для измерения и управления подотчётностью департаментов и служб. См. G. James Herrera, The Fundamentals of Military Readiness, Congressional Research Service at 2 (Oct. 2, 2020), https://fas.org/sgp/crs/natsec/R46559.pdf.

10. Как отмечалось в главе 6 настоящего доклада, уже существует определённая потребность в создании цифрового корпуса, гражданского и военного ИИ и связанных с ним областей карьеры, расширении путей набора персонала и

создании рекрутинговых бюро. Военные службы должны оценивать численность персонала в этих областях и структурах, а не необходимость их создания.

11. Хотя ИИ будет повсеместно распространён во всех областях, большие объёмы данных, связанные с областями космических, кибер-и информационных операций, делают случаи использования в этих областях особенно подходящими для приоритетной интеграции приложений с поддержкой ИИ в военных играх, учениях и экспериментах.

12. Стимулирующий фонд Warfighting Lab предназначен для стимулирования полевых экспериментов и демонстраций, чтобы «оценить, проанализировать и дать представление о более эффективных способах использования существующих возможностей, а также определить новые способы включения технологий в будущие операции и организации.» См. Меморандум Заместителя министра обороны, Фонда стимулирования лаборатории боевых действий и структуры управления Министерства обороны США (6 мая 2016 г.), https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/DSD_memo.pdf.

13. Предполагаемая сеть хорошо согласуется с текущими усилиями Министерства обороны по обеспечению совместимости на основе стандартов, адаптации систем и обмена данными. См. Меморандум Министра Военно-морского флота, министра армии и министра Военно-воздушных сил для руководителей по приобретению услуг и руководителей программ Министерства обороны США (7 января 2019 года). https://www.dsp.dla.mil/Portals/26/Documents/PolicyAndGuidance/Memo-Modular_Open_Systems_Approach.pdf.

14. Такие, как цели и основные направления, изложенные в Стратегии цифровой инженерии Министерства обороны; термины, любые знания и руководящие принципы, разделяемые в рамках Совокупности знаний цифровой инженерии; и включение раздела 231 Закона о разрешении национальной обороны на 2020 финансовый год, который требует создания

возможностей цифровой инженерии для автоматизации тестирования и оценки. См. Стратегию цифровой инженерии Министерства обороны, Офис заместителя помощника министра обороны по системной инженерии (июнь 2018 г.); см. также Pub. L. 116-92, Закон о разрешении национальной обороны на 2020 финансовый год, 133 Stat. 1198 (2019). Описание Совокупности знаний в области цифровой инженерии см. в статье Эндрю Монье, Будущее направление разработки моделей на основе моделей в Министерстве обороны США (27 января 2020 г.), https://ac.cto.mil/wpcontent/uploads/2020/05/RAMS-Monje-27Jan2020-Future.pdf.

15. Подробнее о том, как эта архитектура должна взаимодействовать с цифровой экосистемой, см. в главе 2 «План действий».

Автономные системы вооружения и риски, связанные с войной с использованием искусственного интеллекта

Смягчение стратегических рисков, связанных с системами вооружения с поддержкой искусственного интеллекта

Продолжайте Строгие Процедуры TEVV	Разработка международных стандартов практики
Обсудите риски с конкурентами	Ограничьте Конкретные Области Применения

Мировые военные державы, как большие, так и малые, стремятся к созданию автономных систем вооружения с поддержкой искусственного интеллекта (ИИ).

Такие системы могут помочь командирам принимать более быстрые, эффективные и важные решения.

Они позволят оружейным системам быть способными к уровням производительности, скорости и дискриминации, которые превышают человеческие возможности. И они позволят решать доселе невыполнимые сложные задачи. При правильном проектировании, испытании и использовании они могли бы улучшить соблюдение норм Международного гуманитарного права (МГП) за счет снижения риска случайных столкновений, уменьшения числа жертв среди гражданского населения, минимизации сопутствующего ущерба инфраструктуре и обеспечения возможности детального аудита решений и действий операторов, и их командных цепочек. Хотя американские оружейные платформы используют автономные функции уже более восьми десятилетий, технологии ИИ обладают потенциалом для создания новых, сложных наступательных и оборонительных автономных возможностей.

Растущее использование технологий искусственного интеллекта в системах вооружения породило важные вопросы относительно того, являются ли такие системы законными, безопасными и этичными.

Те, кто критикует использование технологий ИИ в оружии, утверждают, что государства должны вести переговоры об ограничениях или ограничениях на такие системы и их использование.

Существует также озабоченность по поводу того, что автономные системы вооружения могут сделать эскалацию конфликта более вероятной, и продолжаются дебаты о том, какие шаги необходимы для обеспечения того, чтобы такие системы сводили к минимуму риск непреднамеренных военных столкновений или непреднамеренной и неконтролируемой эскалации конфликта.

С 2014 года Конвенция Организации Объединённых Наций о конкретных видах обычного оружия (КОО) проводит совещания между государствами-участниками для обсуждения технологических, военных, правовых и этических аспектов «новых технологий в области смертоносных автономных систем оружия (ЗАКОНОВ)». В частности, она изучает, будут ли автономные технологии способны соответствовать МГП и необходимы ли дополнительные

меры для обеспечения того, чтобы люди сохраняли надлежащую степень контроля над применением силы.

Комиссия консультировалась с гражданским обществом, научными организациями и правительственными учреждениями при изучении правовых, этических и стратегических вопросов, связанных с системами оружия с поддержкой ИИ и автономными системами, включая их потенциальные военные выгоды и риски, возможные этические проблемы, выходящие на первый план, международные усилия по их регулированию и соблюдение МГП.

Комиссия предлагает следующие четыре решения, отражающие её выводы по итогам этих обсуждений.

Решение 1: При условии, что их использование санкционировано командиром или оператором-человеком, должным образом спроектированные и испытанные системы оружия с поддержкой искусственного интеллекта и автономные системы оружия использовались и могут продолжать использоваться способами, совместимыми с МГП. Это суждение основано на нескольких элементах МГП: • Различие: Принцип различия гласит, что стороны в вооружённом конфликте должны проводить различие между гражданскими лицами и комбатантами.4 Оружие со все более точными системами распознавания целей с поддержкой искусственного интеллекта потенциально способно сократить случаи неправильной идентификации целей, что является основной причиной непреднамеренных столкновений во время боевых действий, и тем		Суждения NSCAI Относительно систем вооружения с поддержкой искусственного интеллекта и Автономных систем вооружения • При условии, что их использование санкционировано человеческим командиром или оператором, должным образом спроектированные и испытанные системы оружия с поддержкой искусственного интеллекта и автономные системы оружия использовались и могут продолжать использоваться способами, совместимыми с МГП. • Существующие процедуры МО способны гарантировать, что Соединённые Штаты будут размещать безопасные и надёжные системы вооружения с поддержкой искусственного интеллекта и автономного оружия и использовать их в соответствии с МГП. • Существует мало доказательств того, что американские конкуренты имеют эквивалентные строгие процедуры для

самым уменьшить жертвы среди гражданского населения и сопутствующий ущерб инфраструктуре.5 •Соразмерность: Принцип соразмерности запрещает нападения, которые могли бы привести к случайным потерям гражданских лиц, чрезмерным по сравнению с ожидаемым военным преимуществом.6 Автономные системы вооружения с поддержкой искусственного интеллекта могут и должны также проектироваться для проведения операций в соответствии с человеческими суждениями и указаниями относительно соразмерности нападения.		обеспечения того, чтобы их автономные системы вооружения с поддержкой ИИ были ответственно спроектированы и законно использованы. • Комиссия не поддерживает глобальный запрет систем вооружения с поддержкой искусственного интеллекта и автономных систем вооружения.
Моральные рассуждения, включённые в это исчисление, взвешивание ожидаемого военного преимущества против потенциального вреда гражданскому населению остаются обязанностью человеческого командира.		

• Подотчётность: Обеспечение подотчётности и ответственности командования имеет важное значение для соблюдения МГП.

Человек может и должен нести ответственность за разработку, испытания, использование и поведение любой автономной системы оружия, будь то с помощью оружия или иным образом.

Автономные системы вооружения функционируют в рамках тех же общих параметров, что и системы управления людьми, которые специально разработаны для обеспечения подотчётности за действия и соблюдения МГП. Это ничем не отличается от любой другой системы оружия.8

Комиссия одобряет политику Министерства обороны, которая гласит, что человеческое суждение должно быть вовлечено в принятие решений о лишении человека жизни в вооружённом конфликте.

Вид участия, необходимый для того, чтобы люди оставались ответственными за использование автономных систем оружия, будет варьироваться в зависимости от критичности ситуации во времени, а также от оперативного контекста, обстоятельств и типа задействованных систем оружия.

Государства обязаны разработать процессы, обеспечивающие, чтобы при использовании автономных систем оружия с «... человеческое суждение должно быть вовлечено в принятие решений о лишении человека жизни в вооружённом конфликте» поддержкой искусственного интеллекта полагались на соответствующие уровни человеческого суждения и чтобы люди-операторы таких систем по-прежнему несли ответственность за результаты своего использования.

Человеческая ответственность за результаты смертоносных сражений не обязательно требует человеческого надзора за каждым шагом процесса участия.

Как только человек санкционирует атаку на цель или группу целей, последующие шаги в последовательности атак могут быть выполнены автономно, не отказываясь от ответственности человека.

Точное количество шагов в этой последовательности зависит от технических возможностей системы и контекста и должно учитывать такие факторы, как неопределённость, связанная с поведением системы

и потенциальными результатами, величиной угрозы и временем, доступным для действий.

Например, автономная система вооружения, расположенная в быстро меняющейся среде, такой как городская среда, в течение длительного периода времени, может потребовать более частого разрешения человека для обеспечения достаточной ответственности человека за автономные действия, чем эквивалентная система, работающая в течение аналогичного периода времени в очень предсказуемой и менее населённой среде, например, под водой или в космосе.

Эта логика может и должна быть включена в проектирование, тестирование и оперативное планирование системы. Принимая во внимание эти факторы, когда это возможно и считается необходимым, проекты операций должны включать в себя точки необходимого руководства человека в рамках последовательности автоматизированных действий.

В такие моменты человек должен проанализировать состояние системы и санкционировать свои следующие действия, прежде чем миссия системы может продолжаться.

Общее решение о том, чтобы каждый отдельный шаг в сражении, связанном со смертельным исходом, подвергался явному разрешению со стороны человека, не является ни реалистичным, ни желательным. Действительно, такая политика могла бы вместо этого побудить командиров использовать менее точные, неуправляемые системы оружия, что могло бы привести к большему уровню сопутствующего ущерба.

Решение 2: Существующие процедуры МО способны гарантировать, что Соединённые Штаты будут размещать безопасные и надёжные системы вооружения с поддержкой искусственного интеллекта и автономные системы вооружения и использовать их таким образом, чтобы это соответствовало МГП.

Приверженность Министерства обороны строгим процедурам разработки и использования автономных систем вооружения, а также его приверженность строгим этическим принципам ИИ вселяет уверенность

в том, что оно сможет создавать автономные системы вооружения с поддержкой ИИ, которые используются законно.

МО располагает всеобъемлющими процессами обеспечения того, чтобы применение любого оружия, которое оно применяет, соответствовало МГП, и демонстрирует приверженность работе в рамках МГП, минимизации жертв среди гражданского населения и извлечению уроков из своих ошибок.

Министерство Обороны учредило межведомственную юридическую группу – Рабочую группу Министерства обороны по праву войны для «разработки и координации инициатив и вопросов в области права войны, таких как анализ законности новых средств или методов ведения войны, рассматриваемых компонентами Министерства обороны».

Этот постоянный орган имеет хорошие возможности для изучения последствий для МГП по мере развития технологий с течением времени. Международный комитет Красного Креста (МККК) высоко оценил силу и прозрачность этой системы, включив Соединённые Штаты в число восьми стран, которые имеют «национальные механизмы для рассмотрения законности оружия и которые предоставили МККК документы, устанавливающие эти механизмы».

В дополнение к базовому юридическому обзору Департамент принял специальные меры предосторожности в отношении систем утопического оружия, чтобы обеспечить, чтобы эти системы прошли достаточные испытания и оценку, проверку и валидацию (TEVV).

В 2012 году Министерство Обороны дополнило обширный список руководящих директив и инструкций, касающихся разработки оружия в рамках Департамента, опубликовав Директиву Министерства обороны (DoDD) 3000.09 «Автономия в системах вооружения», которая устанавливает политику Министерства обороны в отношении разработки и использования автономных систем вооружения.

Он требует, чтобы все системы были разработаны «для того, чтобы позволить командирам и операторам осуществлять надлежащий уровень

человеческого суждения о применении силы», и требует, чтобы старшие руководители МО сначала одобрили любое автономное оружие со смертельными возможностями, когда начинается разработка, и снова перед вводом в эксплуатацию. Он также предписывает любому автономному или полуавтономному оружию, которое подвергается пересмотру в своём рабочем состоянии, пройти дополнительные испытания и оценку. DoDD 3000.09 содержит важные определения и базовые требования для таких систем и должен ежегодно пересматриваться по мере развития технологии.

В главе 7 настоящего доклада содержатся конкретные рекомендации о том, как Соединённые Штаты должны адаптировать свою политику и возможности в области ТЭВВ для обеспечения того, чтобы они сохраняли обоснованное доверие к системам с поддержкой искусственного интеллекта.

«Приверженность США МГП является давней, и автономные системы вооружения с поддержкой искусственного интеллекта не изменят этой приверженности.»

Кроме того, процедуры командования и контроля МО, санкционирующие выбор целей и применение боеприпасов, являются строгими и предназначены для обеспечения соблюдения МГП.

Оперативным командирам на местах оказывают непосредственную поддержку юристы, внедрённые на различных уровнях для консультирования по вопросам принятия решений о применении силы. Приверженность США МГП является давней, и автономные системы вооружения с поддержкой искусственного интеллекта не изменят этой приверженности. Эти же принципы будут внедрены в конструкцию этих вооружений, продемонстрированы в TEVV и поддержаны командирами, контролирующими их развёртывание.

Политика Министерства Обороны в отношении автономии в системах вооружений и принятие им этических принципов для ИИ в 2020 году ещё больше подчёркивают и укрепляют эту приверженность.

Суждение 3: Существует мало доказательств того, что американские конкуренты имеют эквивалентные строгие процедуры для обеспечения того,

чтобы их автономные системы оружия с поддержкой искусственного интеллекта были ответственно спроектированы и законно использованы.

Успех на поле боя может стать все более зависимым от производительности ИИ, и оружие с поддержкой ИИ, вероятно, будет распространяться, учитывая открытый исходный код и природу ИИ двойного назначения.

Это может привести к усилению давления на государства с целью быстрого внедрения новых и непроверенных систем и алгоритмов.

Такое давление может также склонить проекты в сторону систем, которые реагируют быстрее, ограничивая количество времени, доступного для эффективного человеческого надзора за решениями по взаимодействию конкуренты, в частности Россия и Китай, вероятно, не имеют эквивалентных оперативных и целевых процедур для обеспечения соответствия использования таких систем МГП и сохранения ответственности человека за применение смертоносной силы.

Россия и Китай также не опубликовали ничего эквивалентного DoDD 3000.09, изложив свою политику и процессы, регулирующие приобретение, разработку, испытания и развёртывание автономных систем вооружения.

В отличие от США, в России и Китае эти процессы являются секретными, если они вообще существуют.

Американские конкуренты продемонстрировали, что они вряд ли будут придерживаться тех же этических и правовых стандартов при разработке и использовании систем оружия с поддержкой искусственного интеллекта. Россия, в частности, исторически демонстрировала готовность к развёртыванию рискованных и недостаточно испытанных систем вооружения, а также развёртывала в боевых действиях в Сирии плохо работающие беспилотные наземные транспортные средства с ограниченными автономными функциями. Китай не только активно добивается расширения автономных функций по «Глобальному договору, запрещающему разработку, развёртывание или использование автономных систем оружия с поддержкой

искусственного интеллекта, в настоящее время не отвечает интересам США или международной безопасности ...»целому ряду военных систем, но и в настоящее время экспортирует вооружённые беспилотные летательные аппараты с автономными функциями в другие страны. Это включает в себя такие системы, как Blowfish A3, который Ziyan, производитель системы, рекламирует как способный проводить автономные, смертельные, целенаправленные удары.

Решение 4: Комиссия не поддерживает глобальный запрет на использование автономных систем оружия с поддержкой искусственного интеллекта.

Глобальный договор, запрещающий разработку, развёртывание или использование автономных систем оружия с поддержкой искусственного интеллекта, в настоящее время не отвечает интересам США или международной безопасности и был бы нецелесообразен по нескольким причинам:

• Во-первых, это основная проблема определения. Что касается автономных систем вооружения, то, хотя обсуждение законов в ООН началось ещё в 2014 году, государства до сих пор не согласовали их определение.

Это делает любые переговоры по договору проблематичными, поскольку может оказаться невозможным определить категорию систем, подлежащих ограничению таким образом, чтобы обеспечить достаточную ясность, не чрезмерно ограничивая существующие военные возможности США.

• Даже если проблема определения может быть преодолена, мы считаем, что в настоящее время осуществление такого соглашения было бы непрактичным, поскольку его соблюдение не может быть проверено.

Нет никакого осуществимого технического способа, с помощью которого государства могли бы продемонстрировать друг другу, что конкретные системы вооружений являются или не являются автономными, или что они обладают или не обладают определёнными возможностями.

Это потребовало бы от иностранных инспекторов быстрого доступа к базовому коду в оружейных системах, вызывающих озабоченность. Государства вряд ли согласятся на такой навязчивый режим проверки, поскольку раскрытие этой информации создаст неприемлемые риски для безопасности их систем.

• Кроме того, последствия соглашения о запрещении, вероятно, будут противоречить стратегическим интересам США.

Обязательства со стороны таких государств, как Россия или Китай, скорее всего, будут пустыми. Такое соглашение не будет служить цели оказания политического давления на государства, которые с наибольшей вероятностью развернут автономные системы вооружений небезопасными и этическими способами. Скорее, основное воздействие соглашения будет заключаться в усилении давления на те страны, которые соблюдают международное право, включая Соединённые Штаты и их демократических союзников и партнёров.

Кроме того, различные взгляды на запрет среди союзников США могут углубить разногласия между ними по поводу использования автономных систем вооружения с поддержкой ИИ. Если союзники США присоединятся к соглашению, в то время как Соединённые Штаты этого не сделают, это расхождение, вероятно, помешает военной совместимости союзников.

По этим причинам мы считаем, что практические и стратегические проблемы, связанные с договором о запрещении, перевешивают потенциальные выгоды для Соединённых Штатов и их союзников и партнёров, и поэтому мы поддерживаем нынешнюю политику США в отношении такого соглашения. Однако это не исключает других соглашений или политики, направленных на устранение стратегических рисков, связанных с системами оружия с поддержкой ИИ и автономными системами оружия, или будущей возможности регулирования конкретных типов технологий в технологиях оружия с поддержкой ИИ и автономных системах оружия, когда такое соглашение может быть поддающимся проверке.

Рекомендации по снижению стратегических рисков ИИ.

Хотя Комиссия считает, что должным образом спроектированные, испытанные и использованные автономные системы оружия с поддержкой искусственного интеллекта принесут существенную военную и даже гуманитарную пользу, бесконтрольное глобальное использование таких систем потенциально чревато непреднамеренной эскалацией конфликтов и кризисной нестабильностью. Соединённые Штаты не могут предполагать, что автономные системы вооружения с поддержкой ИИ, поставляемые другими странами, будут разработаны, приобретены и поставлены на вооружение с соответствующим испытанием и проверкой, чтобы позволить им действовать по назначению. Непреднамеренные эскалации могут происходить по многим причинам, в том числе когда системы не работают должным образом, из-за сложных и непроверенных сложностей взаимодействия между системами оружия с поддержкой ИИ и автономными системами оружия на поле боя, и, в более общем плане, в результате неправильного восприятия сигналов или действий машин или людей.

Системы с поддержкой искусственного интеллекта, вероятно, увеличат темпы и автоматизацию ведения войны по всем направлениям, сократив время и пространство, доступные для деэскалационных мер.

Помимо испытаний и надёжности, мы не можем предполагать, что автономное оружие с поддержкой ИИ, разработанное другими странами, будет спроектировано так, чтобы вести себя в соответствии с МГП.

Поэтому страны должны принимать меры, направленные на снижение рисков, связанных с системами оружия с поддержкой ИИ и автономными системами оружия, и поощрять безопасность и соблюдение МГП при обсуждении их разработки, развёртывания и применения.

Такие усилия должны и должны возглавляться Соединёнными Штатами, которые имеют уникальную возможность руководить ими, учитывая их технический опыт, военную доблесть, а также чёткую и прозрачную политику и

этические принципы, регулирующие развёртывание и использование автономных систем вооружения с поддержкой ИИ.

Комиссия представляет следующие пять рекомендаций относительно действий, которые Соединённые Штаты должны предпринять для снижения рисков, связанных с системами оружия с поддержкой искусственного интеллекта и автономными системами вооружения.

Стратегические риски, связанные с оружием с поддержкой ИИ	Рекомендуемые Действия NSCA Действия США	Цели
Национальные государства могли бы позволить ИИ санкционировать использование ключевых стратегических систем вооружений.	Чётко и публично подтвердите существующую политику США, согласно которой только люди могут санкционировать применение ядерного оружия, и добивайтесь аналогичных обязательств от России и Китая.	Предотвратите непреднамеренный ядерный конфликт из-за разрешения запуска с поддержкой искусственного интеллекта.
Государства не могут проверять соблюдение потенциальных международных соглашений, касающихся оружия с поддержкой ИИ.	Использовать технические средства для проверки соблюдения будущих соглашений о контроле над вооружениями, касающихся систем вооружения с поддержкой ИИ и автономных систем вооружения.	Обеспечить эффективную проверку потенциальных будущих соглашений, что обеспечивает уверенность в том, что системы работают по назначению, не раскрывая конфиденциальных оперативных деталей.
Стратегические риски, связанные с оружием с поддержкой ИИ	Рекомендуемые Действия NSCA	Цели
Глобальное,	Финансировать	Разрабатывайте и

нерегулируемое распространение оружия с поддержкой ИИ и автономного оружия.	исследования по техническим средствам предотвращения распространения систем оружия с поддержкой ИИ и автономных систем вооружения.	внедряйте устойчивые к распространению элементы в сложное автономное оружие с поддержкой искусственного интеллекта и потенциально делитесь ими с Россией и Китаем.
Плохо спроектированное или неправильно использованное оружие может вести себя непредсказуемо.	Действия США с союзниками Разработка международных стандартов практики разработки и использования систем вооружения с поддержкой ИИ и автономных систем вооружения. Установить международные нормы, регулирующие ответственную разработку и использование систем вооружения с поддержкой ИИ и автономных систем вооружения.	Установить международные нормы, регулирующие ответственную разработку и использование систем вооружения с поддержкой искусственного интеллекта и автономных систем вооружения.
Системы с поддержкой	Действия США с	Улучшить понимание

ИИ могут привести к непреднамеренной эскалации конфликта.	Россией и Китаем Обсудите влияние ИИ на кризисную стабильность в существующем российско-американском стратегическом диалоге по безопасности и создайте эквивалентный содержательный диалог с Китаем.	доктрины и разработать меры укрепления доверия в отношении использования систем вооружения с поддержкой искусственного интеллекта и автономных систем вооружения.

Чётко и публично подтвердите существующую политику США, согласно которой только люди могут санкционировать применение ядерного оружия, и добивайтесь аналогичных обязательств от России и Китая. Соединённые Штаты должны сделать чёткое публичное заявление о том, что решения о санкционировании применения ядерного оружия должны приниматься только людьми, а не системой с поддержкой искусственного интеллекта или автономной системой, и должны включить такое подтверждение в следующий обзор ядерной позиции Министерства обороны.

Это укрепило бы и выделило бы существующие США политика, в которой говорится, что «решение о применении ядерного оружия требует явного разрешения Президента Соединённых Штатов».

Это также продемонстрировало бы практическую приверженность США ответственному использованию ИИ и автономных функций, ограничению безответственных возможностей и предотвращению эскалации конфликтов опасными способами системами ИИ.

Это также могло бы иметь стабилизирующий эффект, поскольку уменьшило бы страхи конкурентов перед внезапным ударом Соединённых

Штатов с использованием искусственного интеллекта и могло бы побудить другие страны взять на себя аналогичные обязательства.

Соединённые Штаты также должны активно давить на Россию и Китай, а также на другие государства, обладающие ядерным оружием, чтобы они выступили с аналогичными заявлениями. Хотя совместные политические обязательства о том, что только люди разрешат применение ядерного оружия, не будут поддаваться проверке, они все же могут стабилизироваться, отвечая на классическую дилемму заключённого пока страны уверены, что другие не строят рискованные структуры командования и управления, которые могут непреднамеренно спровоцировать массовую ядерную эскалацию, у них «...страны должны принимать меры, направленные на снижение рисков, связанных с системами оружия с поддержкой ИИ и автономными системами оружия, а также поощрять безопасность и соблюдение МГП при обсуждении их разработки, развёртывания и применения. Такие усилия должны и должны возглавляться Соединёнными Штатами...» будет меньше стимулов для разработки таких систем самостоятельно. Хотя эта норма широко принята в Соединённых Штатах, неясно, разделяют ли Россия и Китай одни и те же стратегические интересы.

Публичные сообщения указывают на то, что Россия ранее установила систему «мёртвой руки» для автоматизации выдачи разрешений на ядерные пуски, а представители Китая в диалогах по Второму направлению с Соединёнными Штатами не решались заявить, что Китай возьмёт на себя аналогичное обязательство.

Если ни Россия, ни Китай не готовы согласиться на такое предложение, США должны развернуть мощную кампанию международного давления, чтобы осудить это решение и подчеркнуть, как Россия и Китай отказываются брать на себя обязательства по ответственному военному использованию ИИ.

Обсудите влияние ИИ на кризисную стабильность в рамках существующего российско-американского диалога по стратегической безопасности (ССБ) и создайте эквивалентный содержательный диалог с

Китаем. Госдепартаменты и Минобороны должны обсудить влияние ИИ на кризисную стабильность в рамках существующих российско-американских отношений и создать эквивалентный содержательный диалог с Китаем.

ССД - это межведомственный двусторонний диалог, направленный на снижение недопонимания и недопонимания по ключевым стратегическим вопросам и угрозам, а также снижение вероятности непреднамеренной эскалации.

Хотя диалог традиционно фокусировался на контроле над ядерными вооружениями и доктрине, в последнее время он используется также для обсуждения новых технологий и космической безопасности.

У Соединённых Штатов нет эквивалентного диалога с Китаем, поскольку Китай почти десять лет сопротивлялся попыткам США установить такой диалог. Однако в течение последнего года появляется все больше свидетельств того, что Китай заинтересован в официальных переговорах с Соединёнными Штатами относительно военных систем с поддержкой искусственного интеллекта. Этот интерес следует культивировать и использовать для создания американо-китайского ССД, включающего в себя соответствующих военных, дипломатических и силовых чиновников с обеих сторон.

Учитывая, что Соединённые Штаты, Россия и Китай все агрессивно преследуют возможности ИИ, и что Россия и Китай, вероятно, выставят системы ИИ, которые прошли менее строгий TEVV, чем сопоставимые американские системы, и могут быть небезопасными или ненадёжными, крайне важно улучшить взаимопонимание военных доктрин друг друга, в том числе в отношении ИИ и автономных систем. Соединённые Штаты должны использовать этот канал, чтобы подчеркнуть, как развёртывание небезопасных систем может привести к непреднамеренной эскалации конфликта, подчеркнуть необходимость проведения строгого TEVV и обсудить, где каждая сторона видит риски быстрой эскалации обычного конфликта, чтобы лучше предвидеть будущие ответные меры в кризисе.

«... крайне важно улучшить взаимное понимание военных доктрин друг друга, в том числе в отношении систем с поддержкой искусственного интеллекта и автономных систем.»

Эти диалоги могли бы также посеять семена для будущего постоянного диалога, направленного исключительно на установление практических и конкретных мер укрепления доверия вокруг автономных систем вооружений с поддержкой искусственного интеллекта. Например, Соединённые Штаты, Россия и Китай могли бы работать над разработкой «международного соглашения об автономных инцидентах» по образцу Соглашения об инцидентах на море 1972 года, которое будет стремиться определить «правила дорожного движения» для поведения автономных военных систем, чтобы создать более предсказуемую операционную среду и избежать аварий и просчетов.

Они также могли бы договориться об интеграции «автоматических растяжек эскалации» в системы, которые предотвратили бы автоматизированную эскалацию конфликта в конкретных сценариях без вмешательства человека, включить использование ядерного оружия, как отмечалось выше.

Рекомендация

Работа с союзниками по разработке международных стандартов практики разработки, тестирования и использования автономных систем вооружения с поддержкой искусственного интеллекта. Соединённые Штаты должны тесно сотрудничать со своими союзниками в разработке стандартов практики в отношении того, как государства должны ответственно разрабатывать, тестировать и применять автономные системы оружия с поддержкой искусственного интеллекта. Это может быть основано на существующей работе, включающей Руководящих принципов, согласованных Группой правительственных экспертов по законам (ГПЭ) в 2019 году29 DoDD 3000.09,

Этические принципы МО для ИИ и Ключевые соображения NSCAI для ответственной разработки и внедрения ИИ.

В рамках этих усилий Рабочая группа МО по праву войны должна регулярно проводить совещания для рассмотрения любых будущих технических разработок, касающихся автономных систем вооружения и МГП, а Руководящий комитет под председательством трёх членов по новым технологиям должен давать рекомендации о том, как такие будущие технические разработки влияют на политику и национальную оборону.

Результаты работы обеих групп должны стать основой для будущих взаимодействий Минобороны как с союзниками, так и с конкурентами по созданию автономных систем вооружения с поддержкой ИИ.

Достижение консенсуса союзников в отношении стандартов разработки, тестирования и использования таких систем установит важные нормы в отношении этих систем, поможет обеспечить их разработку и безопасное использование и ещё больше подчеркнёт приверженность Соединённых Штатов и их союзников этическому и ответственному использованию ИИ.

Соединённые Штаты также должны использовать эти консультации для того, чтобы осветить пути, с помощью которых ИИ станет важной частью будущих военных операций, и разработать общие рамки, определяющие надлежащее и ответственное использование автономных систем оружия с поддержкой ИИ на поле боя.

Это должно стимулировать союзников инвестировать в цифровую модернизацию своих собственных сил, а также подчёркивать риски для военной совместимости, если какой-либо союзник согласится присоединиться к договору, запрещающему ЗАКОНЫ.

Использовать технические средства для проверки соблюдения будущих соглашений о контроле над вооружениями, касающихся оружейных систем с поддержкой искусственного интеллекта. Соединённые Штаты должны активно заниматься разработкой технологий и стратегий, которые могли бы обеспечить эффективную и надёжную проверку будущих соглашений о контроле над

вооружениями, предусматривающих использование технологий искусственного интеллекта. Хотя контроль над вооружениями в отношении систем вооружения, оснащённых ИИ, в настоящее время технически не поддаётся проверке, эффективная проверка, вероятно, будет необходима для достижения будущих юридически обязательных ограничений на возможности ИИ. Министерство обороны и Министерство энергетики должны возглавить усилия по разработке и внедрению технологий, которые могли бы обеспечить другим странам уверенность в том, что автономная оружейная система с поддержкой искусственного интеллекта работает так, как задумано, не раскрывая секретных оперативных деталей. Например, он мог бы изучить способы создания оружейными платформами с поддержкой ИИ аутентичных записей операций, которые можно было бы проверить на месте с помощью международных инспекций по вызову, если возникнут подозрения в несоблюдении требований. Техническое творчество будет необходимо для того, чтобы обеспечить любые будущие международные ограничения возможностей ИИ без раскрытия конфиденциальной информации.

Финансировать исследования по техническим средствам предотвращения распространения систем вооружения с поддержкой ИИ и автономных систем вооружения. Контроль за распространением систем оружия с поддержкой ИИ и автономных систем оружия создаёт значительные проблемы, учитывая открытый исходный код, двойное использование и неотъемлемо передаваемый характер алгоритмов ИИ.

Распространение самодельных автономных систем вооружения, которые в основном используют коммерческие компоненты, будет особенно трудно контролировать с помощью регулирования и потребует эффективного обмена разведывательными данными и внутренних усилий правоохранительных органов по предотвращению их использования террористами и другими негосударственными субъектами.

Что касается более сложных автономных систем вооружения, то Соединённым Штатам следует удвоить усилия по разработке и внедрению

устойчивых к распространению элементов, таких как стандартизированные способы предотвращения использования такого оружия неавторизованными пользователями или перепрограммирование функциональности системы путём изменения ключевых параметров системы.

Минобороны должны финансировать технические исследования по таким методам, и при необходимости эти методы могут быть переданы России и Китаю или, возможно, другим странам для предотвращения распространения или потери контроля над некоторыми автономными системами оружия с поддержкой ИИ.

Настоящий доклад не содержит отдельного Плана действий для Главы 4. Это объясняется тем, что, учитывая важность этой темы, Комиссия решила подробно изложить свои аргументы, рекомендации и конкретные действия, необходимые для их осуществления, непосредственно в этой главе. Кроме того, более подробную информацию о том, как Соединённые Штаты должны адаптировать свою политику TEVV для поддержания доверия к системам ИИ, можно найти в главе 7 и связанном с ней Плане действий, а рекомендации по соответствующим изменениям организационной структуры МО можно найти в главе 3.

Примечания

1 МГП также упоминается как право вооружённых конфликтов (ПВК) и право войны.

2 Paul Scharre, Army of None: Autonomous Weapons and the Future of War, W. W. Norton & Co. at 39 (24 апреля 2018 года).

3 Справочная информация о смертоносных автономных системах вооружения в КОО, Организация Объединённых Наций (последний доступ 11 января 2021 года), https://www.unog.ch/80256EE600585943/(httpPages)/8FA3C2562A60FF81C1257CE600393DF6?OpenDocument.

4 Знак Отличия, Международный комитет Красного Креста (последний доступ 15 января 2021 года), https://casebook.icrc.org/glossary/distinction.

5 Есть возможности для улучшения ситуации с уменьшением ошибочной идентификации целей в ходе военных операций США. Например, во время войны в Афганистане исследование показало, что около половины всех инцидентов с жертвами среди гражданского населения, вызванных американскими войсками, были вызваны неправильной идентификацией целей. Использование систем с поддержкой ИИ для принятия более точных решений о прицеливании, возможно, является основным способом, с помощью которого правильное использование ИИ может сделать войну более гуманной. Ларри Льюис, Redefining Human Control: Lessons from the Battlefield for Autonomous Control, CNA at 4 (March 2018), https://www.cna.org/cna_files/pdf/DRM-2017-U-016281-Final.pdf.

6 Пропорциональность, Международный комитет Красного Креста (последний доступ 15 января 2021 года), https://casebook.icrc.org/glossary/proportionality.

7 См. Paul Scharre, Army of None: Autonomous Weapons and the Future of War, W. W. Norton & Co. at 255-257 (2018).

8 Для правильно спроектированной и испытанной автономной системы, которая правильно выполняет намерение командира, командир несёт чёткую ответственность за действия этой системы. Государства обязаны надлежащим образом разрабатывать, испытывать и использовать такие системы, а также вводить строгие процедуры, обеспечивающие соответствие любого применения оружия МГП, в том числе путём обеспечения индивидуальной ответственности.

9 Комиссия считает, что существующая формулировка МО «соответствующее человеческое суждение», обсуждаемая в следующем Решении, отражает это необходимое изменение и гарантирует, что любое решение о применении смертоносной силы начинается с человеческого суждения и находится под контролем человеческого суждения, и что человек в

конечном счёте будет нести ответственность за любое решение о применении силы.

10 Пресс - релиз Министерства обороны США, Министерство обороны принимает этические принципы искусственного интеллекта (24 февраля 2020 года), https://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adoptsethical-principles-for-artificial-intelligence/.

11 DoDD 5000.01 требует, чтобы любое оружие, выставленное Министерством обороны, проходило юридическую экспертизу для обеспечения соблюдения Права вооружённых конфликтов (LOAC), соблюдая требования, изложенные в статье 36 Дополнительного протокола к Женевским конвенциям от 12 августа 1949 года. Додд 3000.09 и принципы этики собачьего ИИ строятся на этой базовой линии. См. Директиву Министерства обороны 5000.01: Система оборонных закупок, Министерство обороны США от 9 сентября 2020 г., https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/500001p.pdf?ver=2020-09-09-160307-310; Дополнительный протокол к Женевским конвенциям от 12 августа 1949 года, касающийся защиты жертв международных вооружённых конфликтов (Протокол I), 8 июня 1977 года, Международный комитет Красного Креста (последний доступ 5 января 2021 года), https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/WebART/470-750045.

12 Директива Министерства обороны № 2311.01: Программа военного права Министерства обороны США от 11 (2 июля 2020 года), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/231101p.pdf?ver=2020-07-02-143157-007.

13 A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977, International Committee of the Red Cross at 5, n. 8 (Jan. 2006), https://www.icrc.org/en/doc/assets/files/other/icrc_002_0902.pdf.

14 Директива Министерства обороны 3000.09: Автономия в системах вооружения, Министерство обороны США в 2 (21 ноября 2012 г., вкл.

изменение 1 8 мая 2017 года), https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf. Процессы обзора вооружений, установленные в DoDD 3000.09, специально разработаны для обеспечения того, чтобы любая автономная система вооружений США соответствовала таким принципам МГП, как дискриминация и соразмерность, а также поддерживала надлежащий уровень человеческого суждения и обеспечивала подотчетность.

15 Инструкция Министерства обороны 5025.01: Программа выпуска минобороны на 22 (1 августа 2016 г., вкл. изменение 3 22 мая 2019 года), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/502501p.pdf?ver=2020-05-20-081854-657.

16 См. Приложение к настоящему отчёту, содержащее сокращённую версию ключевых соображений NSCAI по ответственной разработке и внедрению ИИ. Дополнительные сведения о рекомендации Комиссии в отношении будущих НИОКР, необходимых для расширения возможностей тестирования, Оценки, верификации и вариации систем искусственного интеллекта, см. в разделе «Производительность системы» в разделе «Ключевые соображения для ответственной разработки и внедрения искусственного интеллекта: Расширенная версия», NSCAI (2021) (имеется в архиве Комиссии).

17 Руководство МО по праву войны служит подробным ресурсом для всего персонала МО, ответственного за осуществление закона войны и проведение военных операций. См. Руководство Министерства обороны по военному праву, Министерство обороны США (декабрь 2016 г.), https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190.

18 Пресс - релиз Министерства обороны США, Министерство обороны принимает этические принципы искусственного интеллекта (24 февраля 2020 года), https://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adoptsethical-principles-for-artificial-intelligence/.

19 Дэвид Экс, Не паникуйте, Но Россия Обучает своих Роботов-Танков понимать Человеческую речь, Forbes (30 июня 2020 года), https://www.forbes.com/sites/davidaxe/2020/06/30/dont-panic-but-russia-istraining-its-robot-tanks-to-understand-human-speech/?sh=7373377914f2.

20 Патрик Такер, SecDef: Китай экспортирует Роботов-убийц на Ближний Восток, Defense One (5 ноября 2019 года), https://www.defenseone.com/technology/2019/11/secdef-china-exporting-killer-robotsmideast/161100/.

21 Соединённые Штаты выразили аналогичную озабоченность в отношении договоров о запрещении кассетных боеприпасов и ядерного оружия. См. Вопросы и ответы: Конвенция по кассетным боеприпасам, HRW (6 ноября 2010 г.), https://www.hrw.org/news/2010/11/06/qa-convention-cluster-munitions#; Хизер Уильямс, Что означает Договор о запрещении ядерного оружия для союзников Америки, Война на скалах (5 ноября 2020 года), https://warontherocks.com/2020/11/what-the-nuclear-ban-treaty-means-for-americas-allies/. По состоянию на март 2021 года ни один союзник, с которым Соединённые Штаты имеют соглашение о взаимной обороне, не выразил поддержки договору о запрете ЗАКОНОВ.

22 Комиссия признает, что ИИ должен оказывать помощь в некоторых аспектах ядерного аппарата командования и управления, таких как раннее предупреждение, раннее обнаружение запуска и многосенсорный синтез для проверки обнаружения отдельных датчиков и потенциального устранения ложных обнаружений.

23 Справочник по ядерным вопросам 2020 года, Канцелярия заместителя помощника министра обороны по ядерным вопросам в 18 (2020), https://fas.org/man/eprint/nmhb2020.pdf.

24 Могут быть и другие причины, по которым страны могут делегировать полномочия на запуск ядерного оружия автономным системам, особенно если руководство доверяет машинам выполнять приказы на запуск больше, чем людям. Политическое соглашение вряд ли сможет решить эти проблемы, хотя

его предложение подчеркнёт, как другие страны ведут себя безответственно и опасно.

25 Майкл Пек, Ядерное оружие Судного дня «Мёртвой руки» России вернулось, Национальный интерес (12 декабря 2018 года), https://nationalinterest.org/blog/buzz/russias-dead-hand-nuclear-doomsday-weaponback-38492.

26 Пресс-релиз Госдепартамента США, Участие заместителя госсекретаря Салливана в Диалоге по стратегической безопасности с заместителем министра иностранных дел России Сергеем Рябковым (17 июля 2019 года), https://2017-2021.state.gov/deputy-secretary-sullivans-participation-in-strategic-securitydialogue-with-russian-deputy-foreign-minister-sergey-ryabkov/index.html; Пресс - релиз Госдепартамента США, США и России Провести обмен космической безопасностью (28 июля 2020 года), https://2017-2021.state.gov/the-united-states-and-russia-hold-space-security-exchange/index.html.

27 За последний год китайские эксперты активно участвовали в нескольких диалогах Track II с американскими экспертами по безопасности военных систем искусственного интеллекта, потенциально сигнализируя о желании официального общения правительства с правительством по этим вопросам.

28 См. Michael C. Horowitz and Paul Scharre, AI and International Stability: Risks and Confidence Building Measures, Center for a New American Security (Jan. 2021), https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/AI-and-International-Stability-Risks-and-Confidence-BuildingMeasures.pdf?mtime=20210112103229&focal=none.

29 Заключительный доклад Сессии Группы правительственных экспертов по новым технологиям в области смертоносных автономных систем оружия 2019 года, Группа правительственных экспертов Высоких Договаривающихся сторон Конвенции о запрещении или ограничении применения конкретных видов обычного оружия, которые могут считаться наносящими чрезмерные повреждения или имеющими неизбирательное действие,

CCW/MSP/2019/CRP.2/Rev. 1, (13-15 ноября 2019 года), https://undocs.org/CCW/MSP/2019/9.

30 См. Приложение к настоящему отчёту, содержащее сокращённую версию ключевых соображений NSCAI по ответственной разработке и внедрению ИИ. Дополнительные сведения о рекомендации Комиссии относительно будущих действий в области международного сотрудничества и сотрудничества см. в разделе «Производительность системы» в разделе «Ключевые соображения ответственного развития и внедрения искусственного интеллекта: Расширенная версия», NSCAI (2021) (имеется в архиве Комиссии).

31 Дополнительную информацию о трудностях использования экспортного контроля для предотвращения передачи алгоритмов искусственного интеллекта см. в главе 14 настоящего доклада.

32 Таким образом, в 1970-х годах Соединённые Штаты поделились с Советским Союзом технологией разрешительных связей (PALs), которые предотвращают несанкционированное вооружение ядерным оружием. Неясно, существует ли эквивалентная технология PALs для ИИ, которая снизила бы риск несанкционированной или случайной эскалации со стороны системы ИИ без одновременного значительного повышения военных характеристик этой системы. Если будут разработаны эквивалентные технологии, то вопрос о сотрудничестве придётся рассматривать в каждом конкретном случае.

ИИ и будущее национальной разведки

2025: Поддержка искусственного интеллекта и анализ

Расширение возможностей научно - технического лидерства	Инновационные подходы к объединению людей и машин
Капитализация ИИ-анализа информации с открытым исходным кодом	Приоритетность сбора научно - технической информации

Построение информационно-технологической среды ИС

Разведка выиграет от быстрого внедрения технологий искусственного интеллекта (ИИ) больше, чем любая другая миссия национальной безопасности.

Поскольку каждая возможная платформа как машинная, так и человеческая вносит свой вклад в глобальную информационную сеть, а число датчиков растёт экспоненциально, объем, скорость и разнообразие данных угрожают подавить интеллектуальный анализ.

Установить достоверность и ценность информации будет сложнее. Перед анализом будет поставлена задача обеспечить контекст, имеющий решающее значение для превращения информации в действенный интеллект.

ИИ поможет специалистам разведки находить иголки в стогах сена, соединять точки и разрушать опасные сюжеты, выявляя тенденции и обнаруживая ранее скрытые или замаскированные признаки и предупреждения. Возможности искусственного интеллекта улучшат каждый этап цикла разведки-от постановки задач до сбора, обработки, эксплуатации, анализа и распространения.

Алгоритмы искусственного интеллекта могут просеивать огромные объёмы данных, чтобы найти закономерности, обнаружить угрозы, выявить корреляции и сделать прогнозы.

Инструменты искусственного интеллекта могут сделать более понятными спутниковые снимки, сигналы связи, экономические показатели, данные социальных сетей и другие крупные источники информации.

ИИ может находить корреляции между данными из открытых источников и другими источниками разведывательной информации и помогать Разведывательному сообществу (ИС) быть более точным, эффективным и результативным в своей деятельности по таргетированию и сбору данных.

Совокупность современных и новых технологий искусственного интеллекта, применимых к разведывательным миссиям, включает в себя компьютерное зрение для анализа изображений, биометрические технологии (такие как распознавание лица, голоса и походки), обработку естественного языка и алгоритмические функции поиска и запросов для больших баз данных.

Самое главное, ИИ позволяет объединять данные из разнородных потоков данных для создания композитной картины.

В военных сценариях против технологически продвинутых противников, государств изгоев или террористических организаций-платформы разведки, наблюдения и разведки с поддержкой ИИ, а также системы индикации и предупреждения (I&W) будут иметь решающее значение для передовых боевых возможностей.

Благодаря автоматизации системы с поддержкой искусственного интеллекта оптимизируют постановку задач и сбор данных для платформ, датчиков и активов в режиме, близком к реальному времени, в ответ на требования динамической разведки или изменения в окружающей среде.

На тактическом фронте «умные» датчики будут способны предварительно обрабатывать необработанные разведданные и определять приоритетность данных для передачи и хранения, что будет особенно полезно в условиях деградации или низкой пропускной способности.

После сбора интеллектуальные системы обработки могут сортировать информацию, выявлять тенденции и закономерности, обобщать ключевые последствия и подготавливать наиболее приоритетную информацию для анализа человеком (или отмечать элементы, представляющие особый интерес, на основе определённых аналитиком условий). Это включает в себя передовые системы ввода-вывода, которые позволят бойцам предвидеть и понимать возникающие угрозы раньше, позволяя им проактивно формировать окружающую среду, а также системы, близкие к тактическому краю, идентифицирующие состязательные усилия по отрицанию и обману.

В сочетании с человеческим суждением эти способности повысят осведомлённость во всех областях, приведут к более жёстким и информированным циклам принятия решений, предложат рекомендации для различных направлений действий и позволят быстро противодействовать действиям противника.

Необходимость адаптации становится насущной в связи с ускоряющимся распространением этих новых технологий. Когда-то изысканные возможности IC теперь широко используются во всем мире.

Способность наших противников быстро внедрять инструменты ИИ означает, что ИС может быть более уязвимой для обмана, информационных операций, раскрытия источников и методов, кибероперациий и контрразведывательной деятельности. IC была одним из первых движителей внутри правительства в создании некоторой базовой инфраструктуры для внедрения ИИ, такой как заключение контракта на создание коммерческого облачного сервиса IC в 2013 году.

Кроме того, инициатива IC 2019 года По расширению интеллекта с использованием машин (AIM) обеспечила направление и основу для более широкого внедрения ИИ, и некоторые разведывательные агентства добились больших успехов в внедрении ИИ, поставив их впереди других в правительстве.

Тем не менее, критические барьеры в органах власти, политике, бюджетах, обмене данными и технических стандартах не позволяют ИС полностью реализовать свой потенциал, и ни одна из этих рекомендаций не будет эффективной без существенных реформ процесса проверки безопасности.

Амбициозная повестка дня: ИИ-Готов к 2025 году.

Чтобы развить прогресс, достигнутый отдельными ведомствами, ИС должна поставить перед собой амбициозную цель внедрения и интеграции возможностей искусственного интеллекта во всех возможных аспектах разведывательного предприятия в рамках более широкого видения будущего разведки.

Уже IC к 2025 году:

Специалисты по разведке обеспечили базовую цифровую грамотность и доступ к цифровой инфраструктуре и программному обеспечению, необходимым для повсеместной интеграции ИИ на каждом этапе цикла разведки.

Начиная немедленно, ИС должна уделять приоритетное внимание автоматизации каждого этапа цикла разведки в максимально возможной степени и обработке всех имеющихся данных и информации с помощью аналитических систем с поддержкой искусственного интеллекта до проведения анализа человеческими аналитиками.

Продукты также должны распространяться с машинной скоростью, что означает, что они должны быть в машиночитаемых форматах-и системы по всей ИС должны быть в состоянии принимать и использовать их без ручного вмешательства.

Оптимизация систем с поддержкой ИИ таким образом потребует совершенно иного подхода к созданию и анализу готовых интеллектуальных продуктов. ИС должна требовать, чтобы все продукты разведки включали как читаемую человеком версию, так и, что не менее важно, автоматизированную

машиночитаемую версию, которая может быть введена в другие аналитические системы по всей ИС.

Все будущие разведывательные системы должны быть оптимизированы для сбора и обработки данных, ориентированных на ИИ.

«ИС должна требовать, чтобы все разведывательные продукты включали как читаемую человеком версию, так и, что не менее важно, автоматизированную машиночитаемую версию, которая может быть введена в другие аналитические системы по всей ИС»

Как только ИС автоматизирует свои процессы в рамках отдельных дисциплин разведки, она должна объединить эти отдельные процессы в непрерывный конвейер анализа разведывательной информации из всех источников, обрабатываемый через объединённую архитектуру постоянно обучающихся аналитических механизмов.

Это трансформационное изменение может привести к пониманию, возникающему в результате объединения человека и машины, которое выходит за нынешние пределы человеческого познания без посторонней помощи.

Такая система внесла бы большую ясность в происходящие события, а также позволила бы проводить более точный и надёжный прогнозный анализ возникающих угроз. По мере того как аналитики все больше доверяют системам с поддержкой искусственного интеллекта, соотношение человеческого и машинного анализа будет все больше склоняться в сторону машин.

Подготовка к 2025 году требует следующих действий:

Расширьте возможности научно-технического лидерства IC. Директор национальной разведки (DNI) должен назначить Директора по науке и технике (S&T) в Канцелярии Директора национальной разведки (ODNI) в качестве Главного технического директора IC (CTO) и поручить ему руководить внедрением IC приложений с поддержкой искусственного интеллекта для решения задач оперативной разведки.

Для этого ICC TO должна осуществлять надзор за стратегией AIM, устанавливать и применять общие технические стандарты и политику, необходимые для быстрого и ответственного масштабирования приложений с поддержкой искусственного интеллекта по всей ИС, а также руководить реформой закупок для обеспечения того, чтобы ИС могла быстро закупать и поставлять системы своим специалистам по разведке. ICC TO следует предоставить дополнительные полномочия для разработки политики и надзора за исследованиями и разработками ИС, разработкой технологий, переходом технологий, соответствующей деятельностью по прототипированию, экспериментам и тестированию разработок.

Измените практику управления рисками, чтобы ускорить внедрение новых технологий. ИС должна сбалансировать технические риски, связанные с внедрением новых технологий в оперативный режим и их быстрым обновлением, с существенными операционными рисками, возникающими в результате не успеваемости, аналогично МО. Регулярные обновления программного обеспечения должны быть максимально автоматизированы. Для облегчения обмена программными средствами между учреждениями стандартом должна быть взаимная аккредитация информационно-технологических систем.

«ИС должна сбалансировать технические риски, связанные с внедрением новых технологий и их быстрым обновлением, с существенным операционными рисками, возникающими в результате не успевания за ними ...»

Для координации этих изменений ОДНИ следует создать Совет старших руководителей по управлению рисками, ориентированный на модернизацию технологий.

Его задача должна состоять в том, чтобы взвесить риски внедрения новых технологий с альтернативными издержками, связанными с их отсутствием.

Его цель должна состоять в том, чтобы обеспечить аналитикам доступ к инструментам, необходимым им для выполнения своей работы.

IC будет нуждаться в поддержке со стороны комитетов по разведке в, Конгрессе-например, в гибком использовании средств в рамках более гибкой структуры разработки программного обеспечения.

Чтобы поддержать аргумент в пользу большей гибкости, ИС должна разработать основанные на данных способы передачи оперативных выгод, а также достоверные оценки риска бездействия.

Улучшить координацию и взаимодействие между ИС и МО. ИС должна настойчиво добиваться автоматизированной интероперабельности с МО для разведывательных операций, проводимых на машинных скоростях. Для этого менеджеры по безопасности и сетевые администраторы должны повысить уверенность в быстром и безопасном обмене данными. ODNI, заместитель министра обороны по разведке и безопасности, и Объединённый центр искусственного интеллекта (JAIC) должны больше координировать связанные с разведкой проекты ИИ, чтобы свести к минимуму дублирование усилий при максимальном использовании общих подходов к разработке потенциала ИИ, тестированию и оценке, развёртыванию, международному взаимодействию, а также политике и органам власти.

Они должны работать вместе над созданием совместимых и совместимых ресурсов и инструментов-таких, как те, которые предусмотрены в экосистеме исследований и разработок в области ИИ, описанной в главе 2 настоящего доклада, и должны создать культуру совместного использования всех возможностей ИИ, когда это возможно.

Извлекайте выгоду из анализа информации с открытым исходным кодом и общедоступной информации с помощью ИИ. ИС должна разработать скоординированный и федеративный подход к применению приложений с поддержкой искусственного интеллекта к разведке с открытым исходным кодом (OSINT) и стремиться интегрировать анализ с открытым исходным кодом в существующие процессы разведки везде, где это возможно в каждой области разведывания.

Приоритетность и ускорение сбора научно - технической информации для лучшего понимания возможностей и намерений противника. Такой сбор требует от ИС значительного повышения технической сложности, возможностей и потенциала её аналитической рабочей силы.

Это должно включать активные усилия по обучению, набору и удержанию аналитиков, обладающих необходимыми навыками.

Эти аналитики должны направлять требования к сбору данных и предоставлять своевременные и точные оценки.

Чтобы лучше координировать разведывательные данные по этим темам, включая сбор информации о научно-техническом сотрудничестве между нашими конкурентами, ДНР должна назначить Ответственного за сбор новых технологий в рамках Национального разведывательного совета.

Чтобы привлечь больше научно-технических экспертов в ИС, настойчиво проводить реформу допуска к секретности на уровне сверхсекретности и выше, а также обеспечивать взаимность допуска секретности среди членов ИС. Следует разработать и внедрить основанный на искусственном интеллекте и научно обоснованный подход к вынесению решений по вопросам безопасности, который значительно сокращает сроки расследования.

Продвигайтесь вперёд и продолжайте развивать специально созданную информационную технологическую среду IC, которая может объединять интеллект из различных областей и источников. Подобная техническая архитектура с поддержкой искусственного интеллекта могла бы помочь автономно интегрировать интеллект между различными областями интеллекта, которые в настоящее время часто требуют ручного вмешательства для обмена необработанными данными или готовым анализом.

Это поможет IC смешать инсайты из различных потоков информации для создания композитной картины.

Например, сигнальный интеллект часто зависит от человеческого интеллекта или непространственного интеллекта.

Точно так же ценность человеческого интеллекта почти всегда может быть повышена путём наслоения на него сигнального интеллекта или информации из открытых источников.

Примите слитый, прогностический анализ как новый стандарт. Успешное слияние интеллекта всех источников и всех доменов позволит провести точный прогнозный анализ таким образом, который в настоящее время невозможен.

Реакция правительства на вирус COVID-19 позволила заглянуть в потенциал слияния наборов данных для такого анализа.

Например, Северное командование США (работающее с JAIC и Бюро Национальной гвардии) построило прогностические модели из десятков различных наборов данных, которые помогли идентифицировать горячие точки COVID-19 и согласовать потребности в критически важных поставках.

Разрабатывайте инновационные человеко-ориентированные подходы к объединению людей и машин. Вид слияния данных, предполагаемый здесь через автономную машинно-машинную интеграцию, потребует новых концепций для объединения человека и машины, которые оптимизируют сильные стороны каждого.

ИС будет нуждаться в новых подходах, которые усиливают и расширяют человеческое познание, чтобы эффективно справляться с масштабом и сложностью информации, генерируемой аналитическими механизмами интеллекта из всех источников.

При разработке этих систем ИС должна понимать и принимать обдуманные решения о том, когда и при каких условиях человек или машина должны действовать в одиночку и при каких условиях желательно объединение человека и машины.

«Вид слияния данных, предполагаемый здесь через автономную машинно-машинную интеграцию, потребует новых концепций для объединения человеко-машин, которые оптимизируют сильные стороны каждого».

Примечания

1. Для получения дополнительной информации о случаях использования ИИ на протяжении всего цикла разведки см. Обсуждение «Приложений» в поддержании интеллектуального превосходства: Переосмысление и изобретение интеллекта с помощью инноваций, CSIS Technology and Intelligence Task Force на 8-22 (13 января 2021 года), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210113_Intelligence_Edge.pdf.

2. AIM Initiative: A Strategy for Augmenting Intelligence Using Machines, Office of the Director of National Intelligence (2019), https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf (предисловие достопочтенной Сью Гордон, первого заместителя директора Национальной разведки).

3. Фрэнк Конкель, Подробности сделки ЦРУ с Amazon, The Atlantic (14 июля 2014 года), https://www.theatlantic.com/technology/archive/2014/07/the-details-about-the-cias-deal-withamazon/374632/.

4. При внедрении новых программных систем ИС руководствуется системой управления рисками, разработанной Национальным институтом стандартов и технологий (NIST). Хотя в целом это полезная структура, она также может создавать задержки или препятствовать тому, чтобы ИС шла в ногу с передовыми инструментами искусственного интеллекта, которые имеются в продаже. Для получения дополнительной информации см. Проект внедрения FISMA, NIST (3 декабря 2020 г.), https://csrc.nist.gov/projects/risk-management/rmf-overview.

5. Совет по управлению старшими рисками будет помогать IC выполнять руководящие указания предлагаемого Комитета трёх председателей по новым технологиям и функционировать аналогично той роли, которую эта комиссия рекомендовала заместителю министра обороны по исследованиям и инженерии в качестве сопредседателя Объединённого совета по надзору за требованиями в МО.

6. Для получения дополнительной информации см. Kent Luneburg, et al., Intelligence After Next: The Future of the IC Workplace, MITRE Center for Technology and National Security (1 ноября 2020 г.), https://www.mitre.org/sites/default/files/publications/pr-20-1891-intelligence-after-next-the-future-of-the-ic-workplace.pdf.

7. Эти усилия должны основываться на Совместном общем фонде JAIC (JCF).

8. Pub. L. 116-260, Сводный закон об ассигнованиях (2021), Раздел W, Раздел 326 («Стратегии и планы разведки с открытым исходным кодом для разведывательного сообщества»), Раздел 623 («Независимое исследование по разведке с открытым исходным кодом») и Раздел 624 («Обзор предприятий с открытым исходным кодом») обеспечивают отправную точку для IC для переосмысления роли разведки с открытым исходным кодом.

9. Важно отметить, что разведка с открытым исходным кодом (OSINT) не ограничивается традиционными источниками ИНФОРМАЦИИ (газеты, радиопередачи и т. Д.) и социальными сетями. OSINT также включает общедоступную информацию, такую как источники данных государственного управления (официальные отчёты, бюджетные документы, свидетельские показания и т. Д.), профессиональные и академические публикации, коммерческие источники данных (отраслевые отчёты, финансовые отчёты, коммерческие изображения и т. Д.) и многое другое.

10. Для получения дополнительной информации см. дискуссию на тему «Повышение технического интеллекта» в Поддержании интеллектуального превосходства: Переосмысление и изобретение интеллекта с помощью инноваций, CSIS Technology and Intelligence Task Force at 12 (Jan. 13, 2021), https://csis-website-prod.s3.amazonaws.com/s3fspublic/publication/210113_Intelligence_Edge.pdf.

11. Для получения дополнительной информации о необходимости академического и научного обзора поведенческих подходов к разрешению вопросов безопасности см. David Luckey, et al., Assessing Continuous Evaluation Approaches for Insider Threats: How Can the Security Position of the US

Departments and Agencies Be Improved?, RAND Corporation at 28-34 (2019), https://www.rand.org/pubs/research_reports/RR2684.html.

12. Технические аспекты такой среды более подробно рассматриваются в главе 2 настоящего доклада.

13. Генерал ВВС Терренс Дж. О'Шонесси, командующий Северным командованием США и армией генерал-лейтенант Лора Дж. Ричардсон, командующий Северной армией США, Стенограмма: Командиры US NORTHCOM и ARNORTH Обсуждают текущие усилия COVID-19, Министерство обороны США (21 апреля 2020 года), https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/2160070/us-northcomand-arnorth-commanders-discuss-ongoing-covid-19-efforts/.

14. См. Kenneth M. Ford, et al., Cognitive Orthoses: Towards Human-Centered AI, AI Magazine at 7 (Winter 2015), https://doi.org/10.1609/aimag.v36i4.2629; John Laird, et al., Future Directions in Human Machine Teaming Workshop, Министерство обороны США (16-17 июля 2019 г.), https://basicresearch. Defense.gov/Portals /61/Будущее%20Directions%20in%20Human%20 Machine%20 Steaming%20 Workshop%20report%20%20%28for%20public%20release%29.pdf; Gagan Bansal, et al., Является ли самый точный ИИ Лучшим товарищем по команде? Оптимизация ИИ для командной работы, AAAI 2021 (февраль 2021), https://www.microsoft.com/en-us/research/publication/is-the-most-accurate-ai-the-best-teammate-optimizing-aifor-teamwork/.

Технические таланты в правительстве

Организовать, набирать, строить, использовать.

Соревнование по искусственному интеллекту (ИИ) выиграет не та сторона, которая обладает лучшими технологиями.

Он будет выигран на стороне лучших, самых разнообразных и технически подкованных талантов. Министерство обороны и Разведывательное сообщество сталкиваются с тревожным дефицитом талантов.

Эта проблема является самым большим препятствием для того, чтобы США существовали уже к 2025 году.

Агентствам национальной безопасности сейчас нужно больше цифровых экспертов, иначе они останутся неготовыми покупать, создавать и использовать ИИ и связанные с ним технологии.

Цифровая экспертиза является наиболее важным требованием для модернизации правительства, но лишь немногие части правительства адекватно инвестировали в создание цифровой рабочей силы.

«Министерство обороны и СК сталкиваются с тревожным дефицитом талантов Министерство обороны и СК сталкиваются с тревожным дефицитом талантов».

Чтобы расширить свою цифровую и искусственную рабочую силу, правительство должно:

• Организация технологов в правительстве с помощью системы управления талантами, предназначенной для размещения высококвалифицированных специалистов;

• Нанимать людей, которые уже обладают необходимыми для правительства навыками, таких как отраслевые эксперты, учёные и недавние выпускники колледжей;

• Создание собственной рабочей силы путём обучения и воспитания нынешних и будущих государственных служащих;

• Более эффективно использовать свою цифровую рабочую силу, чтобы обеспечить цифровым талантам возможность выполнять значимую работу, как только они окажутся в правительстве.

Цифровая экспертиза-это важнейшее требование модернизации государства ...»

Нынешняя Модель.

Правительственные организации, ответственные за создание ИИ – решений, изо всех сил пытаются создать свою цифровую рабочую силу. Реальные препятствия мешают набору и удержанию практиков ИИ и более широких цифровых талантов.

Правительство не конкурирует с зарплатами в частном секторе и страдает от громоздкого процесса найма, а все реформы тормозятся медленным процессом проверки безопасности.

Мы не должны принимать нежелательный статус-кво как неизбежное будущее.

Правительство может конкурировать с частным сектором за таланты. Правительство может не соответствовать зарплатам частного сектора, но оно даёт возможность решать проблемы национальной безопасности и вносить существенный вклад в развитие общества.

Самое большое препятствие, мешающее набору цифровых талантов, это не компетенция. Это восприятие и слишком часто реальность, что цифровым талантам в правительстве трудно выполнять значимую работу с современными вычислительными инструментами на переднем крае быстро меняющейся области.

«Мы не должны принимать нежелательный статус-кво как неизбежное будущее. Правительство может конкурировать с частным сектором за таланты.»

Комиссия не убеждена аргументом о том, что правительство должно сосредоточиться на управлении проектами, сборе и управлении данными и передать всю разработку на аутсорсинг.

Мы слышали этот аргумент от лидеров, которые не верят, что правительство может нанять или обучить своих собственных экспертов по ИИ. Интересно, что мы не слышали этого аргумента от промышленности.

«Правительственные стратегии, которые не развивают государственную техническую рабочую силу, являются недальновидными.»

Государственные учреждения, которые полагаются исключительно на подрядчиков для цифровой экспертизы, станут неспособными понять лежащую в основе технологию достаточно хорошо, чтобы принимать успешные решения о приобретении независимо от подрядчиков.

Такая ситуация создаёт риски для национальной безопасности.

В то время как подрядчики должны продолжать играть важную роль, они стимулируются и в некотором смысле обязаны выполнять условия своего контракта, а не стремиться к общему совершенствованию системы или не соглашаться с плохо продуманными требованиями или неэффективными стратегиями.

В результате агентства, которые полагаются на подрядчиков, вынуждают своих цифровых экспертов иметь второстепенный голос в ключевых решениях, даже связанных с их областью знаний. У правительства всегда будут подрядчики. Но правительство может и должно развивать собственную цифровую рабочую силу.

То, как организована цифровая рабочая сила, так же важно, как и уровень её квалификации. Для создания и управления квалифицированной цифровой рабочей силой в масштабах, требуемых предприятием национальной безопасности, правительству необходимо создать систему управления талантами, адаптированную к этой задаче.

Департаменты и отдельные агентства должны создать Цифровой корпус. Мы предлагаем, чтобы департаменты и отдельные агентства создавали Цифровой корпус, который набирал бы и обучал персонал, размещал людей и управлял цифровой карьерой, устанавливал стандарты квалификации цифровой рабочей силы. Департаменты и отдельные агентства будут создавать пулы для членов этих Цифровых корпусов и давать им указания о работе, которую они выполняют для агентств.

Модель Цифрового корпуса вдохновлена Армейским Медицинским корпусом, который организует специалистов со специализированными медицинскими навыками, которые не вписываются в традиционную систему

управления талантами армии. Как и Медицинский корпус, специализированный Цифровой корпус агентства должен иметь специализированную кадровую политику, руководящие принципы продвижения по службе, учебные ресурсы и сертификаты для демонстрации мастерства в новых цифровых областях.

Чтобы заполнить эти Цифровые корпуса и улучшить свою более широкую цифровую рабочую силу, правительству необходимо улучшить набор персонала и процесс найма, ускорить проверку безопасности, использовать временные средства найма, такие как Закон о межправительственном персонале, и создать механизмы для неполной гражданской службы.

Многие специалисты в области искусственного интеллекта и других цифровых технологий заинтересованы в работе с правительством в качестве штатных или неполных сотрудников.

Из тех, кто хочет работать полный рабочий день, некоторые ищут всю карьеру в качестве государственного гражданского лица или в армии.

Другие менее склонны брать на себя долгосрочные обязательства и вместо этого хотят стать временными, штатными сотрудниками, стипендиатами, участниками обмена талантами или военными резервистами. Третья группа готова работать с правительством или на правительство неполный рабочий день, но они не желают становиться штатными гражданскими служащими и не имеют желания служить в армии.

Создать гражданский национальный резервный цифровой корпус. Правительство должно задействовать пул технологов, готовых посвятить часть своего времени государственной службе, создав механизм их найма. Хотя сотрудники, занятые неполный рабочий день, не могут заменить штатных сотрудников, они могут помочь улучшить образование в области искусственного интеллекта, выполнить сортировку и сбор данных, помочь руководить проектами и разрабатывать цифровые решения, построить мосты между государственным и частным секторами и взять на себя другие важные задачи.

Чтобы устранить этот разрыв в наборе персонала, правительство должно создать гражданский национальный резервный цифровой корпус (NRDC) по образцу обязательств и структуры стимулов военного резерва. Члены NRDC станут гражданскими специальными государственными служащими в одном из Цифровых корпусов агентства и будут работать не менее 38 дней в году в качестве советников, инструкторов или разработчиков по всему правительству.

Оптимизируйте процесс найма и расширьте цифровые конвейеры талантов. Проблемы государственной системы найма хорошо известны: она движется слишком медленно, борется за привлечение экспертов на конкурентном рынке и затрудняет приём на работу молодых или не имеющих учёной степени специалистов, особенно с зарплатой, соответствующей их уровню квалификации.

Эти проблемы не вызваны отсутствием органов по найму или изначально медленным процессом найма. Комиссия не смогла выявить пробел в полномочиях по найму цифровой рабочей силы.

Чтобы устранить это узкое место в рекрутинге, правительству необходимо расширить научно-технический, инженерный и математический (STEM) и искусственный интеллект-трубопроводы талантов из университетов на государственную службу, упростить процесс найма и создать специализированные агентства и военные службы по набору цифровых талантов либо для Цифровых корпусов, либо для агентств. Рекрутинговые бюро будут следить за потребностью своего корпуса, агентства или службы в конкретных типах цифровых талантов и будут иметь возможность набирать технологов виртуально, посещая конференции и ярмарки вакансий, рекрутинг в кампусах колледжей, проведение призовых конкурсов и предлагая стипендии, бонусы за рекрутинг и реферальные бонусы.

Постоянный цифровой корпус будет следить за общегосударственным прогрессом и давать рекомендации по расширению и улучшению найма цифровых талантов и трубопроводов. Они также должны иметь возможность экспериментировать с новыми властями.

Правительство не сможет найти выход из своего технологического дефицита рабочей силы. ИИ и цифровые таланты просто слишком редки в Соединённых Штатах. В 2020 году в Соединённых Штатах было открыто более 430 000 рабочих мест в области компьютерных наук, в то время как только 71 000 новых учёных-компьютерщиков ежегодно заканчивают американские университеты. Правительство также должно взять на себя новые обязательства по созданию своей рабочей силы с нуля с помощью крупной инициативы.

«Соединённым Штатам необходимо создать новую академию обслуживания для обучения будущих государственных служащих цифровым навыкам, необходимым для модернизации правительства.»

Соединённым Штатам необходимо создать новую академию обслуживания для обучения будущих государственных служащих цифровым навыкам, необходимым для модернизации правительства. Академия цифровых услуг США (USDSA) будет аккредитованным университетом, предоставляющим дипломы, который получает как государственное, так и частное финансирование, управляется специально созданным независимым агентством в рамках федерального правительства и удовлетворяет потребности правительства в цифровой экспертизе-как это определено межведомственным советом при содействии Федерального консультативного комитета, состоящего из лидеров частного сектора и академических технологий. Министерство сельского хозяйства США должно быть смоделировано по образцу пяти американских компаний, академии военной службы, но выпускают подготовленных и образованных государственных гражданских лиц для всех федеральных правительственных ведомств и агентств.

«Талантливые люди, работающие в цифровой сфере, должны иметь возможность разумно рассчитывать на то, что они проведут свою карьеру,

выполняя значимую работу, ориентированную на их область знаний в правительстве.»

Талантливые в цифровом плане люди должны иметь возможность разумно рассчитывать на то, что они проведут свою карьеру, выполняя значимую работу, ориентированную на их область знаний в правительстве. Без таких ожиданий они вряд ли присоединятся к правительственной рабочей силе, и без их опыта, соответствующего ожиданиям, они вряд ли останутся надолго. Согласование ожиданий и опыта для цифровой рабочей силы требует трёх изменений:

• Возможность для технологов провести всю свою карьеру, сосредоточившись на той области, которой они увлечены;

• Хорошо информированные лидеры, некоторые из которых сами владеют цифровыми технологиями;

• Доступ к инструментам, наборам данных и инфраструктуре.

Эти изменения более тактические, чем описанные выше, но не менее действенные. Стратегические инициативы преуспевают или терпят неудачу на тактическом уровне, и многие цифровые инициативы, которые в противном случае могли бы иметь стратегическое влияние, борются или терпят неудачу тактически отчасти потому, что правительство не использует своих технологов эффективно.

Создайте новые области цифровой карьеры. Новые сферы профессиональной деятельности ставят под сомнение определение организацией её необходимых компетенций и, возможно, характер её идентичности.

Если военные службы создадут поле для карьеры разработчиков программного обеспечения и специалистов по обработке данных, это почти неизбежно изменит то, что значит быть солдатом, моряком, лётчиком или морским пехотинцем, как это было сделано

Правительство должно создать гражданские профессиональные серии для разработки программного обеспечения, разработки программного обеспечения, управления знаниями, науки о данных и искусственного интеллекта.

Военные службы должны создавать карьерные поля в области разработки программного обеспечения, науки о данных и искусственного интеллекта, как с управленческими, так и со специализированными направлениями. Цифровой корпус будет нуждаться в дополнительных карьерных полях по мере своего развития, но эти шаги создадут прочную основу.

Расширьте доступ к инструментам, наборам данных и инфраструктуре. Высококвалифицированным технологам, работающим в правительстве, регулярно отказывают в доступе к инструментам разработки программного обеспечения. Цифровая рабочая сила нуждается в доступе к программному обеспечению корпоративного уровня наравне с возможностями частного сектора.

Возможности включают в себя инструменты разработки программного обеспечения, доступ к библиотекам программного обеспечения, проверенную поддержку с открытым исходным кодом, кураторские наборы данных и инфраструктуру для крупномасштабного сотрудничества.

Все сферы профессиональной деятельности нуждаются в улучшенном доступе к новейшим библиотекам и инструментам с открытым исходным кодом.

Наиболее продвинутые библиотеки искусственного интеллекта и машинного обучения (мл) нуждаются в огромных объёмах, данных, доступных для обучения моделей.

Предоставление практикам ИИ богатых наборов данных по физическим и биологическим наукам, экономике и поведенческим исследованиям позволит им сосредоточиться на своих областях знаний, а не на поиске неясных источников данных.

Примечания

1. Есть очаги превосходства в нескольких частях правительства, таких как Цифровая служба Соединённых Штатов, Kessel Run, Целевая группа по искусственному интеллекту армии, ускоритель искусственного интеллекта ВВС США-MIT, компоненты Разведывательного сообщества и национальные лаборатории, но их слишком мало, и они недостаточно широко распространились по всему правительству. Требования агентств к размеру и типу рабочей силы ИИ различны, но каждое агентство, привлечённое NSCAI, выразило потребность в расширении своей рабочей силы ИИ, и рекомендации здесь широко применимы.

2. Обсуждения сотрудников NSCA с Советом по оборонным инновациям и Оборонной цифровой службой (май 2019 года).

3 Уильям А. Ла Планте, владеющий Технической базой, Defense AT&L at 18-20 (июль-август 2015 г.), https://apps.dtic.mil/dtic/tr/fulltext/u2/1016084.pdf.

4. Для получения дополнительной информации о Законе о межправительственном персонале см. Закон о межправительственном персонале, OPM (последний доступ к нему был получен 1 февраля 2021 года), https://www.opm.gov/policy-data-oversight/hiring-information/intergovernment-personnel-act/.

5. Code.org (последний раз обращался 11 января 2021 года), https://code.org/promote. См. Также Орен Эциони, Чего не хватает Исполнительному указу Трампа об ИИ: Америке нужна специальная визовая программа, направленная на привлечение большего числа экспертов и специалистов по ИИ, Wired (13 февраля 2019 года), https://www.wired.com/story/what-trumpsexecutive-order-on-ai-is-missing/.

6. В частности, TensorFlow является одной из самых популярных в мире библиотек для обучения нейронных сетей и других алгоритмов машинного обучения (мл). Pitch-это еще одна библиотека с открытым исходным кодом, которая помогает трансформировать исследовательские прототипы в готовые к производству модели машинного обучения.

Установление обоснованного доверия к системам ИИ

Оправдана Уверенность в адаптации и полевом ИИ.

Подотчётность и управление, руководство, прочный и надёжный ИИ, взаимодействие и объединение людей и ИИ, тестирование и оценка, верификация и валидация (TEVV).

Системы искусственного интеллекта (ИИ) должны разрабатываться и применяться с обоснованной уверенностью. Если системы ИИ работают не так, как задумано, или непредсказуемы таким образом, что могут иметь значительные негативные последствия, то лидеры не будут их принимать, операторы не будут их использовать, Конгресс не будет их финансировать, а американский народ не будет их поддерживать.

«Если системы ИИ ... непредсказуемыми способами, которые могут иметь значительные негативные последствия, тогда лидеры не будут их принимать, операторы не будут их использовать, Конгресс не будет их финансировать, а американский народ не будет их поддерживать»

Достижение приемлемой производительности ИИ часто связано с решением принять определённый уровень риска. Ни одна технология не работает идеально при любых условиях.

Расчёт риска меняется в зависимости от обстоятельств.

Переменные и соображения, которые влияют на суждения о том, чтобы полагаться на ИИ, будут значительно различаться в военных, разведывательных, национальных и правоохранительных миссиях.

В условиях высокой угрозы, таких как боевые действия, в некоторых случаях может быть разумно использовать систему, предлагающую некоторое немедленное военное преимущество, признавая при этом, что она может потерпеть неудачу; в других случаях, однако, разумный командир, возможно,

хотел бы получить самые высокие гарантии надёжности ИИ, прежде чем выставлять их на поле, когда жизни людей находятся под угрозой.

«Поскольку департаменты и агентства все больше полагаются на машины, центральным руководящим принципом во всех сценариях национальной безопасности является сохранение центральной роли человеческого суждения.»

Поскольку департаменты и агентства все больше полагаются на машины, центральным руководящим принципом во всех сценариях национальной безопасности является сохранение центральной роли человеческого суждения.

Те, кому поручено использовать ИИ, нуждаются в осознанном понимании рисков, возможностей и компромиссов. Они нуждаются в осознании возможностей и ограничений в ожидаемой производительности системы.

В конечном счёте, им необходимо сформулировать грамотный ответ на этот вопрос: в данных обстоятельствах, насколько уверенности в машине достаточно? Эти вопросы затрагивают весь жизненный цикл системы ИИ от приобретения или разработки системы и пороговых значений обоснованной уверенности в развёртывании конкретной системы с интенсивной ИИ до производительности системы в полевых условиях.

Хотя абсолютной уверенности в совершенстве нет, существуют политика и лучшие практики, которые поддерживают ответственное принятие этих решений.

Агентства в целом осознают основные проблемы, связанные с использованием систем искусственного интеллекта, и необходимость включения передового опыта в разработку и управление системами искусственного интеллекта.

Комиссия подготовила подробную основу для руководства ответственной разработкой и внедрением ИИ в рамках сообщества национальной безопасности (см. Приложение о Ключевых соображениях ответственной разработки и внедрения ИИ).

Он содержит ключевые соображения для политиков и технических практиков, охватывающие весь жизненный цикл ИИ.

Эта система включает рекомендуемые методы, которые должны быть интегрированы и обновлены по мере развития технологии.

Комиссия с удовлетворением отмечает, что некоторые департаменты уже приняли меры по интеграции рекомендаций из нашей рамочной программы.

Чтобы помочь агентствам в выполнении базовых критериев ответственного ИИ, мы выделяем основные проблемы и ключевые рекомендации в нашей структуре по пяти проблемным областям.

1. Прочный и надёжный ИИ.

Современные системы искусственного интеллекта, такие как те, которые используются для восприятия и классификации, имеют различные виды отказов, характеризующиеся частотой ложных срабатываний и ложных отрицаний.

Они часто хрупки, когда работают на грани своей компетенции, и трудно предвидеть границы их компетенции. Они также уязвимы для атак и могут проявлять нежелательную предвзятость в работе.

Для миссий национальной безопасности это может быть серьёзной проблемой:

Сосредоточьте больше федеральных инвестиций в НИОКР на повышении безопасности и надёжности ИИ. Эти инвестиции также должны способствовать интерпретируемости и объяснимости систем искусственного интеллекта, чтобы пользователи могли лучше понять, работают ли эти системы так, как задумано.

Консультируйтесь с междисциплинарными группами экспертов для проведения оценки рисков, совершенствования практики документирования и построения общей архитектуры системы для ограничения последствий сбоя системы. Такие архитектуры должны надёжно контролировать производительность компонентов и обрабатывать ошибки при обнаружении аномалий; содержать компоненты ИИ, которые являются самозащитными (проверка входных данных) и самоконтролируемыми (проверка данных,

передаваемых остальной части системы); и включать агрессивное стресс-тестирование.

«Правительству нужны системы искусственного интеллекта, которые расширяют и дополняют человеческое понимание и принятие решений, чтобы взаимодополняющие сильные стороны людей и ИИ могли быть использованы в качестве оптимальной команды. Достижение этой цели остаётся сложной задачей.»

Взаимодействие человека и ИИ и объединение в команду.

Правительство нуждается в системах ИИ, которые расширяют и дополняют человеческое понимание и принятие решений, так что взаимодополняющие сильные стороны людей и ИИ могут быть использованы в качестве оптимальной команды.

Достижение этой цели остаётся сложной задачей.

Например, люди склонны как к чрезмерному доверию, так и к недоверию машинам в зависимости от контекста.

Существуют также проблемы с измерением производительности команд ИИ, передачей достаточного количества информации, избегая при этом когнитивной перегрузки, позволяя людям и машинам понять обстоятельства, в которых они должны передавать контроль друг другу, и поддержанием соответствующего участия человека для сохранения ситуационной осведомлённости и осмысленного принятия мер, когда это необходимо. Агентствам также необходимо будет определить стандарты работы машин и их ожидания по сравнению с людьми.

Проводите устойчивую, междисциплинарную инициативу через исследовательские лаборатории национальной безопасности для улучшения взаимодействия человека и ИИ. Эта инициатива должна быть направлена на максимизацию преимуществ взаимодействия человека и ИИ, лучшее измерение производительности и возможностей человека при работе с системами ИИ, включая тестирование через непрерывный контакт и эксперименты с

конечными пользователями; и помощь системам ИИ лучше понять контекстуальные нюансы ситуации.

Уточните политику в отношении человеческих ролей и функций, разработайте проекты, оптимизирующие взаимодействие человека и машины, и обеспечьте непрерывное и общеорганизационное обучение ИИ.

Сегодня общий объем инвестиций в RDT&E по областям исследований, 2015-2025 финансовый год

На этом рисунке показаны предполагаемые уровни расходов Министерства обороны по пяти основным категориям исследований, разработанным комиссарами NSCAI, что указывает на то, что инвестиции в взаимодействие человека и ИИ отстают от других категорий исследований.

Примечание уровни расходов, представленные на рисунке, представляют собой оценки, основанные на анализе бюджетных документов Министерства обороны RDT&E на 2021-2025 финансовый год. См. Анализ инвестиций DoD RDT&E в AI, NSCAI (по окончательному согласованию с Комиссией).

Из-за присущих исходным данным проблем с качеством представленные оценки содержат значительные, трудно поддающиеся оценке пределы погрешности.

3. Тестирование и оценка, Верификация и валидация (TEVV).

Оправданное доверие к системам ИИ требует гарантий того, что они будут работать так, как задумано, в том числе при взаимодействии с людьми и другими системами. TEVV традиционных унаследованных систем недостаточно для обеспечения этих гарантий.

В результате агентствам не хватает общих показателей для оценки надёжности систем искусственного интеллекта.

Чтобы свести к минимуму проблемы с производительностью и непредвиденные результаты, потребуется совершенно новый тип TEVV. Это приоритетная и сложная задача. Федеральное правительство должно будет

увеличить инвестиции в НИОКР, чтобы улучшить наше понимание того, как проводить ИИ и связанные с программным обеспечением TEVV. К этой цели:

Dog должна адаптировать и развивать кадровую политику и возможности для удовлетворения изменений, необходимых для ИИ, поскольку системы с поддержкой ИИ растут в количестве, масштабах и сложности в Отделе.

Это должно включать в себя создание структуры и культуры TEVV, интегрирующей непрерывное тестирование; повышение доступности инструментов и возможностей TEVV в рамках Министерства обороны; обновление или создание живых, виртуальных и конструктивных тестовых диапазонов для систем с поддержкой искусственного интеллекта; а также реструктуризацию процессов, лежащих в основе требований к проектированию, разработке и тестированию систем.6

Национальный институт стандартов и технологий (NIST) должен предоставлять и регулярно обновлять набор стандартов, показателей эффективности и инструментов для обеспечения квалифицированной уверенности в моделях ИИ, данных и учебных средах, а также прогнозируемых результатах. NIST должен возглавить сообщество ИИ в создании этих ресурсов, тесно взаимодействуя с экспертами и пользователями из промышленности, научных кругов и правительства, чтобы обеспечить их эффективность.

Лидерство.

Ответственная разработка и внедрение ИИ требует, чтобы конечные пользователи и старшие руководители были осведомлены о возможностях и ограничениях системы, чтобы они не использовались неправильно.

Он также требует, чтобы эксперты по предмету поддерживали обучение, приобретение, оценку рисков и принятие лучших практик по мере их развития.

Сегодня только Министерство обороны имеет специальное руководство ответственным ИИ; сотрудники органов национальной безопасности, выполняющие эти функции, как правило, делают это на добровольной, неполной основе.

Без штатного преданного делу персонала учреждениям не удастся в полной мере внедрить и внедрить эти рекомендуемые методы. Правительство должно:

Назначьте на полный рабочий день ответственного руководителя ИИ высшего уровня в каждом департаменте или агентстве, имеющих решающее значение для национальной безопасности, и в каждом подразделении вооружённых сил. Такое должностное лицо должно руководить ответственным обучением ИИ, предоставлять экспертные знания по ответственной политике и практике ИИ, руководить межведомственной координацией и формировать политику закупок.

Создать постоянный орган междисциплинарных экспертов в Национальном офисе инициативы по ИИ.

Постоянный орган будет предоставлять консультации учреждениям по мере необходимости по ответственным вопросам ИИ.

В группу должны входить люди, обладающие опытом в области ИИ и других областях, таких как этика, право, политика, экономика, когнитивные науки и технологии, включая методы состязательного ИИ.

Подотчётность и управление.

Конгресс и общественность должны видеть, что правительство способно вовремя выявлять и устранять критические недостатки в системах, предотвращать непреднамеренные катастрофы и привлекать людей к ответственности, в том числе за неправильное использование.

Агентства нуждаются в возможности контролировать работу ИИ по мере запуска систем (чтобы оценить, работают ли они так, как задумано) и создавать системы с необходимыми для этого приборами.

Департаменты и агентства, имеющие решающее значение для национальной безопасности и надзорных органов, все выражают проблемы с видимостью своих систем, в то время как поставщики призывают к ясности требований к приборам/проверяемой. Государственные учреждения должны:

Адаптировать и расширить существующую политику подотчётности, чтобы охватить весь жизненный цикл систем искусственного интеллекта и их компонентов.

Разработать политику, позволяющую отдельным лицам выражать озабоченность по поводу безответственного развития ИИ, и внедрить всеобъемлющую практику надзора и правоприменения. Они должны включать требования к аудиту и отчётности, механизм обзора наиболее чувствительных или высокорискованных систем ИИ, а также процессы обжалования и рассмотрения жалоб для тех, кто пострадал от действий систем ИИ.

Примечания

1. Термин «обоснованная уверенность», взятый из широко используемого международного стандарта, использует конкретное определение уверенности как «основания для обоснованной уверенности».» Он отмечает, что «заинтересованные стороны нуждаются в основаниях для обоснованного доверия, прежде чем зависеть от системы» и что «чем выше степень зависимости, тем больше потребность в сильных основаниях для доверия.» ISO/IEC/IEEE International Standard – Systems and Software Engineering – Systems and Software Assurance, IEEE/ISO/IEC 15026-1 (2019), https://standards.ieee.org/standard/15026-1_Revision-2019.html.

2. Подкомитеты Объединённого центра искусственного интеллекта Министерства обороны (JAIC) по ответственному ИИ и тестированию и оценке провели значительные картографические учения, чтобы определить, какая существующая практика соответствует рекомендациям, содержащимся в Ключевых соображениях. Рекомендации, вытекающие из Ключевых соображений, также подкрепляются включениями в Стратегию ИИ Министерства внутренней безопасности (DHS). См. Стратегию искусственного интеллекта Министерства внутренней безопасности, DHS (Dec. 2020), https://www.dhs.gov/publication/us-department-homeland-securityartificial-intelligence-strategy?topic=intelligence-and-analysis.

3. Как и другие интеллектуальные системы, включая программное обеспечение и людей, системы ИИ имеют ограничения на компетентность. Однако у нас меньше науки, чтобы понять ограничения производительности систем искусственного интеллекта, включая причины, когда и как они терпят неудачу.

4. Такие междисциплинарные группы должны изучить возможность документации/ярлыков, определяющих узкую задачу/миссию, для которой была разработана и испытана система. Как отмечается в Приложении о ключевых соображениях ответственной разработки и внедрения ИИ, документация жизненного цикла ИИ должна включать информацию о данных, используемых для обучения и тестирования модели, и методах, используемых для тестирования модели, как на основе контекста, в котором она будет использоваться. Он также должен включать требования к повторному тестированию, переподготовке и настройке, когда система используется в другом сценарии или настройке.

5. Мониторинг может добавить уровень надёжности, но сам по себе также должен быть защищён, чтобы предотвратить новые возможности для внешнего шпионажа или вмешательства в системы ИИ.

6. Модернизация цифровой инфраструктуры, описанная в главе 2 настоящего доклада, потребуется для расширения физических тестовых диапазонов для создания цифровых тестовых сред, которые могут использовать цифровые близнецы.

7. Случаи, в которых добавляются новые датчики и приборы, также могут привести к появлению новых уязвимостей. Особенно важно обеспечить, чтобы общая архитектура таких систем была защищена от внешнего шпионажа и вмешательства.

8. Как отмечалось выше, Комиссия считает, что к ним, как минимум, относятся Министерство обороны, IC, DHS, ФБР, DoE, Государственный департамент и HHS.

9. Подробнее о важности оценки воздействия систем ИИ на права человека см. Доклад Специального докладчика Генеральной Ассамблеи по вопросу об ИИ и его влиянии на свободу мнений и их свободное выражение, Управление Верховного комиссара ООН по правам человека (2018), https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/ReportGA73.aspx.
Пример оценки риска в области прав человека для ИИ в таких категориях, как недискриминация и равенство, участие в политической жизни, неприкосновенность частной жизни и свобода выражения мнений, см. в книге Марка Латонеро «Управление искусственным интеллектом: Защита прав человека и достоинства», Data Society (октябрь 2018 г.), https://datasociety.net/wp-content/uploads/2018/10/DataSociety_Governing_Artificial_Intelligence_Upholding_Human_Rights.pdf.

10. Они могут включать в себя повторные идентификационные атаки. Департаменты и агентства должны использовать средства защиты конфиденциальности, такие как надежная анонимизация, способная противостоять сложным атакам повторной идентификации, и, когда это возможно, технологии сохранения конфиденциальности, такие как дифференциальная конфиденциальность, федеративное обучение и мл с шифрованием данных и моделей.

11. Примерные вопросы оценки рисков, которые использовала IARPA, см. Ричард Данциг, Технологическая рулетка: Управление потерей контроля по мере того, как многие военные стремятся к технологическому превосходству, Центр новой американской безопасности в 22 (28 июня 2018 г.), https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-Technology-Roulette-DoSproof2v2.pdf?mtime=20180628072101.

12. Такая документация должна подкреплять гарантии подлинности, целостности и происхождения данных.

13. См. Создание ответственного ИИ Нормой, а не исключением, Монреальский институт этики ИИ в 9 (13 января 2021 года),

https://arxiv.org/pdf/2101.11832.pdf [далее Отчёт MAIEI] (Это включает в себя «создание отказоустойчивых сейфов и режимов резервного копирования, которые не должны полагаться на непрерывный доступ к» интеллектуальным «элементам и имеют изящные отказы, минимизирующие вред»).

14. См. Brian Wilder, et al., Learning to Complementate Humans, Proceedings of the Twenty Ninth International Joint Conference on Artificial Intelligence (2020), https://www.ijcai.org/Proceedings/2020/0212.pdf.

15. Пример применимых руководящих принципов см. в Saleema Amershi, et al., Guidelines for Human-AI Interaction, CHI ’19: Proceedings of the CHI Conference on Human Factors in Computing Systems (May 2019), https://dl.acm.org/doi/10.1145/3290605.3300233.

16. Подробнее об обучении см. Приложение к настоящему отчёту, содержащее сокращённую версию Ключевых соображений NSCAI по ответственной разработке и внедрению ИИ. Дополнительные сведения о рекомендации Комиссии по обучению см. в разделе «Взаимодействие человека и искусственного интеллекта и объединение усилий» в разделе «Ключевые соображения ответственного развития и внедрения искусственного интеллекта: Расширенная версия», NSCAI (2021) (имеется в архиве Комиссии).

17. Такое повседневное взаимодействие и непрерывные циклы обратной связи будут ещё больше усиливать TEVV.

18. См. Приложение к настоящему отчёту, содержащее сокращённую версию Ключевых соображений NSCAI по ответственной разработке и внедрению ИИ. Дополнительные сведения о рекомендации Комиссии по обучению см. в разделе «Взаимодействие человека и искусственного интеллекта и объединение усилий» в разделе «Ключевые соображения ответственного развития и внедрения искусственного интеллекта: Расширенная версия», NSCAI (2021) (имеется в архиве Комиссии).

Защита демократических ценностей: Неприкосновенность частной жизни, гражданские свободы и гражданские права при использовании ИИ в интересах национальной безопасности

Демократическая модель управления ИИ;

Повышение Общественной Прозрачности;

Инвестируйте в инструменты ИИ и внедряйте их для улучшения надзора и Аудита;

Разработка и тестирование систем обеспечения конфиденциальности и справедливости;

Укрепление Механизмов Надзора;

Защита Правовой защиты и надлежащей правовой процедуры.

Основной целью американского правительства является защита безопасности и свободы американского народа.

У американцев есть давняя традиция обсуждать, как лучше всего достичь этих двух целей, когда между ними возникает напряжённость.

В течение двух десятилетий после 11 сентября были предприняты интенсивные усилия по калибровке полномочий правительства, чтобы остановить ещё один террористический акт с его обязательствами уважать права и свободы личности.

Искусственный интеллект (ИИ) открывает новую эру этой дискуссии, потому что новые технологии предлагают правительственным учреждениям более мощные способы сбора и обработки информации, отслеживания поведения и движений людей и действий на основе компьютерного анализа.

Помимо поддержки военных и разведывательных миссий за рубежом, эти инструменты перспективны для целей национальной безопасности ближе к дому будь то изучение внешней разведки для выявления признаков опасности для Соединённых Штатов, проверка угроз на границах, защита от кибератак и

информационных операций или выявление внутренних террористических заговоров.

Американцы опасаются, что ИИ приложения, используемые в этих целях безопасности и общественной безопасности, особенно те, которые связаны с биометрическими технологиями или анализом агрегированных персональных данных, будут вторгаться в их частную жизнь, ограничивать их свободу слова и собраний и усиливать предвзятость и дискриминацию.

В то же время, при эффективном применении ИИ может помочь улучшить защиту частной жизни и гражданских свобод.

Машинный анализ мог бы быть более точным, а системы искусственного интеллекта потенциально могли бы усилить надзор за помощью мониторинга в реальном времени.

Для Соединённых Штатов, как и для других демократических стран, использование ИИ должностными лицами должно соответствовать принципам ограниченной государственной и индивидуальной свободы.

Эти принципы сами себя не поддерживают. В демократическом обществе любое расширение полномочий государства должно сопровождаться разумными ограничениями, чтобы сделать эту власть легитимной в глазах его граждан.

Как утверждается в этом докладе, перспектива новых технологий искусственного интеллекта для повышения национальной безопасности реальна и значительна.

Необходимо сохранить способность американских спецслужб, органов внутренней безопасности и правоохранительных органов разрабатывать и использовать их в целях национальной безопасности.

Однако для этого правительство должно обеспечить, чтобы их использование было эффективным, законным и законным. Общественное доверие будет зависеть от обоснованной уверенности в соблюдении неприкосновенности частной жизни, гражданских свобод и гражданских прав.

Демократическое управление ИИ и Новые вызовы для частной жизни, гражданских свобод и гражданских прав.

С появлением новых моделей техно-авторитарного управления, набирающих силу за рубежом, Соединённые Штаты должны продолжать служить маяком демократических ценностей. Демократическая модель должна доказать свою устойчивость перед лицом новых технологических изменений, которые могут бросить ей вызов.

По сути, мы уверены, что американская система и правила, нормы и институты, которые её поддерживают могут адаптироваться для поддержания двойственных императивов безопасности и свободы в эпоху искусственного интеллекта.

Для Разведывательного сообщества (IC) основные функции этой системы включают законы, правила и процедуры, позволяющие свести к минимуму сбор, хранение и распространение данных о лицах США, а также надзор со стороны всех трёх ветвей власти.

Органы национальной безопасности и правоохранительные органы также действуют в рамках политики, надзора и судебного надзора, которые руководят охраной границ и уголовными расследованиями.

В конечном счёте действия всех федеральных органов подчиняются гарантиям Конституции.

В этом контексте появление современного ИИ и новых возможностей, которые он может принести разведке, национальной безопасности и правоохранительным миссиям вызывает ряд проблем и сложных вопросов и проблем в отношении частной жизни, гражданских свобод и гражданских прав граждан США:

Аналитика, основанная на ИИ, может помочь чиновникам обрабатывать и осмысливать огромные объёмы информации, которые могут быть объединены для формирования «мозаичной» картины деятельности человека, его местонахождения и моделей поведения.

Объединение разрозненных потоков данных, включающих геолокацию, просмотр веб-страниц, финансовые операции и другие источники данных, создаёт возможность получения новых знаний для аналитиков или исследователей.

Это может быть очень полезно для выявления угроз, но это также поднимает вопросы о надлежащем объёме и разрешении проведения пограничных или правоохранительных поисков.

• Большая часть этой личной информации хранится частными компаниями. Этот факт современной цифровой жизни поднял конституционные вопросы о том, должны ли люди иметь «разумное ожидание конфиденциальности» в информации, которую они предоставляют третьим лицам, таким как технологические фирмы, и вопросы об обстоятельствах, при которых эта информация может быть получена и использована разведкой, национальной безопасностью или правоохранительными органами в законных целях национальной безопасности.

• ИИ может помочь автоматизировать аспекты сбора и анализа данных. Такие методы могут усилить способность аналитиков или исследователей просеивать и сортировать массу информации, чтобы установить закономерности или точно определить угрозы. Но они также поднимают вопросы о надлежащей роли машинного и человеческого анализа в этих процессах, в том числе для принятия прогнозных суждений. В той мере, в какой функции системы ИИ непрозрачны, может быть трудно проследить и обосновать вычислительный процесс, который привёл систему к рекомендации. Определение того, когда и как полагаться на алгоритмы, особенно актуально для минимизации и запросов процедур в СК, а также для построения дел для правоохранительных действий.

• Модели ИИ могут развиваться на основе изменяющихся данных и взаимодействия с другими моделями, что приводит к неожиданным результатам. В результате системы ИИ требуют более непрерывного тестирования и оценки, чем технологии предыдущих поколений.

• Непреднамеренная предвзятость может быть введена на многих этапах процесса машинного обучения (ОД), что может привести к несопоставимым последствиям в американском обществе-проблема, которая была задокументирована в контексте правоохранительных органов.6

Принципы управления вызовами ИИ.

Эта Комиссия не будет пытаться провести все границы того, что может быть допустимо или разумно в конкретных обстоятельствах. Однако важные принципы, которым следует следовать в различных контекстах национальной безопасности, включают следующее:

Сбор и анализ иностранной разведки: Руководство по этике ИИ Управления директора национальной разведки (ODNI) для разведывательного сообщества является обнадёживающим шагом, поскольку оно уделяет большое внимание использованию ИИ для миссий иностранной разведки таким образом, чтобы поддерживать частную жизнь и гражданские свободы американцев.

По мере реализации этих руководящих принципов важно будет уделять пристальное внимание обеспечению того, чтобы процедуры минимизации, хранения и запроса данных были адекватными и строго соблюдались.

Пограничная безопасность: возможности наблюдения и анализа ИИ могут сделать операции правительства более эффективными и действенными на границах и в портах въезда.

Но чтобы поддерживать общественную поддержку такого использования, Министерство внутренней безопасности (DHS) должно позаботиться о том, чтобы автоматизированные процессы проверки приводили агентов только к той информации, которая им нужна и к которой они имеют право доступа, и не позволяли недопустимо выделять отдельных лиц по таким признакам, как раса или религия.

Внутренняя безопасность и общественная безопасность: Быстрое развитие технологий с использованием искусственного интеллекта для правоохранительных целей, включая методы биометрического наблюдения,

такие как распознавание лиц, может опережать правила их надлежащего использования.

Правительство должно проявлять особую осторожность при управлении рисками, связанными с основополагающими конституционными принципами, включая равную защиту, надлежащую правовую процедуру, свободу от необоснованных обысков и арестов, а также свободу слова и собраний.8

При осуществлении этих миссий важно будет проводить чёткие различия между соответствующими органами власти в этих различных контекстах национальной безопасности.

Также важно завоевать большее доверие общественности путём повышения прозрачности, повышения эффективности и надёжности технологий искусственного интеллекта, обеспечения надлежащей правовой процедуры и усиления надзора.

С учётом этих принципов правительство должно предпринять следующие шаги.

Агентства должны оценить краткосрочные возможности и исследовать пробелы в применении ИИ для решения проблем конфиденциальности и гражданских свобод ...»

Инвестируйте и внедряйте инструменты искусственного интеллекта для усиления надзора и аудита в поддержку конфиденциальности и гражданских свобод. Агентствам следует оценить краткосрочные возможности и пробелы в исследованиях применения ИИ для решения проблем конфиденциальности и гражданских свобод, таких как методы ОД для классификации, рекомендации, обнаружения аномалий и другие приложения.9 Примеры достижений в области ИИ для улучшения аудита включают инструменты, поддерживающие финансовый аудит и модельное управление рисками. Учреждениям следует изучить полезность этой и других существующих или возникающих практик.

Повышение общественной прозрачности в отношении того, как правительство использует ИИ. Существует отсутствие прозрачности в политике

и процедурах агентства, а также в точности систем искусственного интеллекта, которые могут повлиять на гражданские свободы. Характер «чёрного ящика» некоторых систем мл только добавляет этой непрозрачности. Повышение прозрачности могло бы помочь облегчить общественные проблемы. Конечно, в определённых оперативных контекстах, особенно для разведывательных и правоохранительных органов, секретность имеет важное значение для миссии. Однако существующие механизмы транспарентности можно было бы использовать более эффективно, а в некоторых случаях и пересмотреть. Новые требования к отчётности агентства также были бы полезны.

• Для систем ИИ, оказывающих влияние на американских граждан, Конгресс должен требовать от Разведывательного сообщества, Министерства внутренней безопасности и Федерального бюро расследований Отчётов об оценке рисков ИИ и Оценок воздействия ИИ. Они должны оценивать последствия конфиденциальности, гражданских свобод и гражданских прав для каждой квалифицируемой системы ИИ или значительного обновления системы.

• DHS и ФБР также должны улучшить практику выдачи уведомлений о системе учёта и оценки воздействия на частную жизнь, чтобы обеспечить более целостное представление о роли систем искусственного интеллекта до их внедрения.

Разрабатывайте и тестируйте системы с целью обеспечения сохранения конфиденциальности и справедливости. Системы ОД, в частности, требуют постоянной оценки гарантий конфиденциальности и справедливости, включая конкретное определение предполагаемой справедливости.

Хотя система мл может удовлетворять требованиям в статический момент времени, постоянное соответствие не является само собой разумеющимся, как только система начинает функционировать.

Это в значительной степени связано с изменением данных, введением непреднамеренной предвзятости и потенциальной повторной идентификацией анонимизированных данных.

Это сложная техническая область, и для достижения большего консенсуса по техническим подходам к сохранению частной жизни, гражданских свобод и гражданских прав требуется продолжение работы в технической, правовой и политической областях.

Между тем агентствам следует предпринять несколько шагов:

• Оценка и смягчение рисков при проектировании, разработке и тестировании систем ИИ. В дополнение к проведению оценки рисков для частной жизни, гражданских свобод и гражданских прав граждан США, IC elements, DHS и ФБР должны принять меры по снижению этих рисков и документировать оставшиеся риски, которые принимаются. При этом они должны использовать методы, основанные на Ключевых соображениях, включая использование средств защиты конфиденциальности, таких как надёжная анонимизация, и, когда это возможно, технологии сохранения конфиденциальности; принятие мер по смягчению предвзятости при разработке и тестировании; и оценка эффективности модели на постоянной основе.

• Определите офис, комитет или группу в каждом агентстве, которые будут проводить предварительный обзор технологий ИИ, влияющих на неприкосновенность частной жизни, гражданские свободы и гражданские права. Это должно включать проверку перед их развёртыванием и на предмет соответствия требованиям в течение всего срока службы системы. В каждом элементе IC, DHS и ФБР должен быть оборудован офис для оценки данных, моделей и системной документации, а также для оценки результатов тестирования систем в отношении их предполагаемого использования.

• Создание сторонних центров тестирования систем ИИ, связанных с национальной безопасностью, которые могли бы повлиять на американских граждан. Такое независимое, стороннее тестирование может быть проведено национальной лабораторией, Университетским исследовательским центром или финансируемым из Федерального бюджета научно-исследовательским центром. Такое тестирование должно быть обязательным для систем с высокими ставками, но в остальном добровольным.17 Она предоставит

учреждениям дополнительные экспертные знания, которые помогут преодолеть внутренние ограничения.

Укрепление способности тех, кто пострадал от действий правительства, связанных с ИИ, добиваться возмещения ущерба и соблюдения надлежащей правовой процедуры.

Системы искусственного интеллекта будут делать ошибки.

Агентства должны принимать ненулевые ложноположительные и ложноотрицательные ставки, чтобы развернуть любую систему искусственного интеллекта. Важно обеспечить возможности для возмещения ущерба в соответствии с конституционным принципом надлежащей правовой процедуры например, когда системная ошибка приводит к отказу в выплате пособия (например, разрешение на визу); ограничениям на передвижение (например, включение в беспилотный список); или арест.

Существуют также проблемы надлежащей правовой процедуры в тех случаях, когда ИИ вносит свой вклад в разработку дела для предъявления уголовных обвинений.

Мы рекомендуем два шага для начала решения этих проблем:

• Пересмотр политики и практики DHS и ФБР, которые могут повлиять на надлежащую правовую процедуру и способность добиваться возмещения ущерба. DHS и ФБР должны пересмотреть политику и практику агентства, чтобы гарантировать, что стороны, пострадавшие от действий правительства, связанных с технологией ИИ, в том числе в результате системных действий или неправильного использования, могут добиваться возмещения ущерба и чётко знать, как это сделать. Этот обзор должен включать в себя вопрос о том, предоставляется ли соответствующим сторонам адекватное уведомление об использовании ИИ в процессе принятия решений, а также степень, в которой системы ИИ могут быть подвергнуты аудиту для отслеживания процесса, с помощью которого система пришла к рекомендации, если она оспаривается.

• Издать руководство Генерального прокурора по ИИ и надлежащей правовой процедуре. В руководстве должно быть описано, как

соответствующие ведомства должны защищать процессуальные права граждан США, когда использование ИИ может привести к лишению жизни или свободы.

Укрепление механизмов надзора для решения текущих и меняющихся проблем. Развитие ИИ требует перспективного подхода к надзору, который предвосхищает дальнейшую эволюцию и внедрение новых технологий и позволяет правительству более ответственно управлять их занятостью в будущем.

«Развитие ИИ требует перспективного подхода к надзору, который предвосхищает дальнейшую эволюцию и внедрение новых технологий, а также лучше позиционирует правительство для ответственного управления их занятостью в будущем.»

Правительство должно:

• Создать целевую группу для оценки последствий ИИ и новых технологий для частной жизни и гражданских свобод. Цель целевой группы состояла бы в выявлении пробелов и выработке рекомендаций по обеспечению того, чтобы использование ИИ и связанных с ним данных в операциях правительства США соответствовало американским законам и ценностям, а также в изучении организационных реформ, которые способствовали бы достижению этой цели. В частности, он должен оценить существующие политические и правовые пробелы в существующих приложениях искусственного интеллекта и новых технологиях и вынести рекомендации по: о законодательные и нормативные реформы в области разработки и использования ИИ и новых технологий и связанных с ними данных; и о институциональные изменения для обеспечения постоянной оценки и постоянного руководства по вопросам конфиденциальности и гражданских свобод, связанных с применением ИИ и новых технологий.

• Укрепить способность Совета по надзору за неприкосновенностью частной жизни и гражданскими свободами (PCLOB) обеспечивать значимый

надзор и консультации по использованию ИИ в интересах национальной безопасности.

С момента своего создания в 2007 году, следуя рекомендации Комиссии 9/11, ПКЛОБ играет особенно важную роль в надзоре и консультировании правительства по вопросам контртеррористических миссий США.

В последние годы она начала обращать внимание на использование новых технологий в сборе и анализе внешней разведки. Совет директоров должен иметь представление о системах ИИ до их внедрения, в том числе на более детальном техническом уровне, и должен быть обеспечен ресурсами и персоналом для выполнения более технически сложной миссии, которая сейчас требуется в эпоху ИИ.

• Расширить возможности Управления DHS по вопросам конфиденциальности, гражданских прав и гражданских свобод (CRCL). Главный сотрудник CRCL в координации с Сотрудником по вопросам конфиденциальности должен играть неотъемлемую роль в юридических процессах и процессах утверждения закупок и использования систем с поддержкой искусственного интеллекта, в том числе связанных с ними данных, используемых в системах DHS мл.

• Требуют более тесной координации и согласования действий между федеральными надзорными и аудиторскими организациями. Соблюдение учреждениями требований к документации и тестированию ИИ должно подкрепляться строгим, технически обоснованным надзором.

Для достижения этой цели и преодоления существующих препятствий в области аудита и надзора постоянный орган должен согласовывать и координировать усилия по усилению надзора и аудита ИИ в отношении неприкосновенности частной жизни, гражданских свобод и гражданских прав.

ПОБЕДА В ТЕХНОЛОГИЧЕСКОМ КОНКУРСЕ

Стратегия конкуренции и сотрудничества

Организация правительства США для решения возникающих технологических проблем;

Создание Совета по конкурентоспособности технологий;

Разработка Национальной технологической стратегии;

Установить высокоуровневый Американо-Китайский научно-технический диалог.

Влияние искусственного интеллекта (ИИ) на мир будет распространяться далеко за пределы узких областей применения национальной безопасности.

Развитие ИИ представляет собой новый столп стратегической конкуренции и усиливает конкуренцию в существующих столпах.

Страна с наиболее устойчивой и производительной экономической базой будет иметь наилучшие возможности для захвата мантии мирового лидерства. Эта база все больше зависит от силы инновационной экономики, которая, в свою очередь, будет зависеть от ИИ. Технологии ИИ будут стимулировать волны прогресса в критической инфраструктуре, торговле, транспорте, здравоохранении, образовании, финансовых рынках, производстве продуктов питания и экологической устойчивости.

Гонка за исследованиями, разработкой и внедрением ИИ и связанных с ним технологий уже усиливает стратегическую конкуренцию.

Правительство США должно принять конкуренцию ИИ и организоваться, чтобы выиграть её. Американский подход к инновациям, который хорошо служил стране на протяжении десятилетий, должен быть пересмотрен, чтобы учесть центральную роль конкуренции с участием ИИ и связанных с ними технологий в формирующемся соперничестве США и Китая. Чтобы сохранить своё инновационное лидерство и позиции в мире, Соединённые Штаты нуждаются в более сильной технологической стратегии под руководством правительства, которая интегрирует политику поощрения и защиты и связывает

инвестиции в ИИ с более широким кругом связанных с ними новых технологий.1

«Гонка за исследованиями, разработкой и внедрением ИИ и связанных с ним технологий уже усиливает стратегическую конкуренцию. Правительство США должно принять конкуренцию ИИ и организоваться, чтобы выиграть её.»

В этой главе излагается природа конкуренции ИИ и две предпосылки для её победы: организация технологической конкуренции под руководством Белого дома и установление принципов дальнейшего сотрудничества с конкурентами.

В следующих главах (10-16) перечисляются основные элементы комплексной стратегии и предписываются действия, направленные на то, чтобы Соединённые Штаты выиграли конкурс ИИ и заложили основу для победы в более широком технологическом соревновании.

Это прежде всего позитивная повестка дня для роста и привлечения талантов, продвижения разнообразной инновационной экосистемы ИИ и инвестирования в НИОКР для использования ИИ и связанных с ним технологий для построения более здорового, процветающего и безопасного общества. Защита исследований, интеллектуальной собственности (ИС) и инвестиций будет необходима в дополнение к усилиям по повышению конкурентоспособности ИИ внутри страны и созданию коалиции единомышленников-партнёров по всему миру.

Правительство Соединённых Штатов должно понять и определить технологическую конкуренцию, организовать её и установить условия для взаимодействия с Китаем.

Конкуренция ИИ между США и Китаем серьёзна и сложна.

Ведущие индексы, измеряющие прогресс в развитии ИИ, обычно ставят США впереди Китая.

Однако разрыв быстро сокращается. У Китая есть разумные шансы обогнать Соединённые Штаты в качестве ведущего центра инноваций в области искусственного интеллекта в ближайшее десятилетие.

В последние годы технологические фирмы в Китае создали новаторские достижения в области обработки естественного языка, технологии распознавания лиц, и других областях с поддержкой искусственного интеллекта.

Китайские бизнесмены, инвесторы, технологи и учёные являются неотъемлемой частью глобального развития ИИ.

Китайские социальные сети и компании электронной коммерции конкурируют за пользователей по всему миру. Их телекоммуникации строят глобальную инфраструктуру 5G.

Её венчурные капиталисты и крупные технологические фирмы вкладывают огромные суммы в новые стартапы, а ведущие компании в области искусственного интеллекта имеют исследовательские лаборатории в США и других странах.

Китайские исследователи создают пласт уважаемых работ по искусственному интеллекту, которые продвигают эту область.

Всё это не касается нас с точки зрения национальной безопасности, за исключением того факта, что Китай возглавляет однопартийный авторитарный режим, угрожающий американским интересам.

«У Китая есть разумные шансы обогнать Соединённые Штаты в качестве ведущего центра инноваций в области искусственного интеллекта в ближайшее десятилетие.»

Китай двигается быстрее и с большей решимостью, чем Соединённые Штаты, руководствуясь созвездием планов ИИ для правительственных министерств, университетов, и компании.

Эти стратегические документы отражают мнение Пекина о том, что достижения в области ИИ коренным образом изменят военную и экономическую конкуренцию в ближайшие десятилетия.

Китай подкрепил свои стратегические планы значительными государственными субсидиями технологическим фирмам и академическим

институтам, занимающимся передовыми исследованиями в области искусственного интеллекта.

Китай сохраняет свой капитал, используя преимущества фундаментальных исследований, проводимых Западом, чтобы он мог больше сосредоточиться на прикладных разработках. Он вкладывает значительные суммы денег в исследования и таланты в соответствующих областях,а также способствует тому, чтобы компании – «национальные чемпионы» завоёвывали рынки за рубежом.

С помощью своих программ военно-гражданского слияния Китай стремится интегрировать достижения в области ИИ из коммерческого и академического миров в военную мощь. Используя шпионаж, программы передачи технологий и целевые инвестиции, Пекин стремится приобрести чувствительные ИС и данные из Соединённых Штатов и других стран.

Конкуренция между США и Китаем осложняется сложной сетью цепочек поставок, исследовательских партнёрств и деловых отношений, которые связывают двух мировых лидеров ИИ.

Драматические шаги по разрыву этих связей могут дорого обойтись американцам и отразиться на всём мире. Отношения между американскими и китайскими учёными, инноваторами и рынками являются глубокими, часто взаимовыгодными и помогают продвигать ИИ. Более того, он остаётся в США.

Национальный интерес заключается в том, чтобы использовать формальный дипломатический диалог об ИИ и других новых технологиях и исследовать области для совместных проектов ИИ, которые принесут пользу человечеству.

«Соединённые Штаты могут конкурировать с Китаем, не прекращая совместных исследований ИИ и не разрывая всю торговлю технологиями.»

Соединённые Штаты могут конкурировать с Китаем, не прекращая совместных исследований ИИ и не разрывая всю торговлю технологиями.

Широкая технологическая развязка с Китаем может лишить американские университеты и компании дефицитных талантов в области искусственного интеллекта, науки, техники, инженерии и математики (STEM),18 а также разрыв эффективных цепочек поставок американских компаний19 и отрезать доступ к рынкам и капиталу для инновационных фирм.20 Вместо этого Соединённым Штатам следует рассматривать целенаправленное распутывание технологических цепочек как один из элементов своего общего подхода, который, если его разумно применять к ключевым секторам, может помочь повысить технологическую устойчивость США, уменьшить угрозы от незаконной передачи технологий и защитить критически важные для национальной безопасности секторы.

Политические вызовы.

Конкурентный подход Китая не должен определять американский подход к инновациям, но он представляет альтернативную модель развития ИИ, определяет ставки конкуренции и раскрывает широту выбора государственной политики, который правительство США должно сделать, чтобы сохранить американские преимущества.

Соединённым Штатам придётся пересмотреть свою иммиграционную политику, чтобы Америка выиграла конкурс на таланты в области искусственного интеллекта. Ей необходимо будет рассмотреть ИИ и более широкие инициативы в области образования STEM через призму глобальной конкурентоспособности. Также ей придётся рассмотреть вопрос о том, как диверсифицировать программу исследований ИИ и расширить доступ к данным и инструментам, необходимым для проведения исследований ИИ, в условиях роста затрат на вычислительные ресурсы и данные, которые консолидируют ИИ в меньшем количестве мест и смещают баланс с университетов на частный сектор.

Соединённым Штатам придётся рассмотреть вопрос о том, насколько давние подходы к ИС лучше всего подходят для эпохи, когда кража ИС широко

распространена и режим ИС США ещё не полностью учитывает ИИ и другие новые технологии.

Соединённым Штатам необходимо будет защитить своё лидерство в разработке микроэлектроники, что может включать в себя поощрение внутренней перестройки критически важных производств, от которых зависит национальная безопасность.

И Соединённые Штаты должны будут обеспечить, чтобы их инструменты и политика, направленные на предотвращение незаконной передачи технологий, были направлены на решение проблем национальной безопасности, связанных с новыми технологиями двойного назначения.

Эти специфические проблемы ИИ, в свою очередь, обнажают ещё более фундаментальные вопросы, охватывающие сферу технологий, экономики и национальной безопасности: • Как конкурировать с соперником, не ставя под угрозу ценности США, включая принципы свободного рынка, свободу личности и ограниченное правительство. • Как обеспечить надлежащий баланс между оборонными и экономическими приоритетами. • Как сохранить преимущества оборудования, не задушив	• Как привлечь лучшие мировые таланты, не допуская вредной передачи технологий и знаний конкурентам. • Как создать открытую среду для совместных исследований, закрывая законные и незаконные лазейки, используемые иностранными конкурентами. • Как поддерживать долгосрочные стратегии НИОКР, которые, тем не менее, реагируют на быстро меняющиеся геополитические и технологические события. • Как обеспечить свободный поток инвестиций/капитала, не позволяя

отечественных конструкторов и производителей, которые полагаются на рынки зарубежных конкурентов. • Как капитализировать и формировать развитие частного сектора для целей национальной безопасности, не подавляя инновации, возглавляемые частным сектором и свободным рынком.	стратегическим конкурентам купить стратегическое преимущество. • Как взаимодействовать с нашими союзниками и другими партнёрами, чтобы уменьшить их зависимость от цифровых технологий Китая, построить более устойчивые цепочки поставок и разработать технологические стандарты и нормы, отражающие демократические ценности.

Необходимость усиления роли государства в технологической стратегии.

Комиссия не призывает к государственной экономике, пятилетнему плану или китайскому «военно-гражданскому слиянию.» Вместо этого она призывает к тому, чтобы возглавляемый правительством процесс восстановил более сбалансированное равновесие между правительством, промышленностью и академическими кругами, которое обеспечивает разнообразную исследовательскую среду, конкурентоспособную экономику и поддержку исследовательской программы, поддерживающей потребности нации.

Правительство имеет долгую историю мобилизации промышленности и научных кругов и делает огромные инвестиции, когда Соединённым Штатам бросают вызов. На фоне такого объявленного и преданного конкурента, как Китай, и учитывая трансформационный потенциал ИИ, Соединённые Штаты сталкиваются с таким моментом.

«... правительство США отстаивает лидерство ИИ в речах и меморандумах, но использует мало ресурсов по сравнению с коммерческими

инвестициями и историческими контрольными показателями финансирования ...»

Сегодня правительство США выступает за лидерство ИИ в выступлениях и меморандумах, но оно использует мало ресурсов по сравнению с коммерческими инвестициями и историческими контрольными показателями финансирования и полагается на децентрализованную структуру управления для его достижения.

Говорят о глобальном конкурсе талантов, но в последние годы Соединённые Штаты ужесточили ограничения на визы для высококвалифицированных рабочих. В США, учащиеся от детского сада до 12-го класса (К-12) отстали от восточноазиатских и европейских конкурентов на экзаменах, предназначенных для измерения компетентности в области STEM.24 Американские эксперты предупреждают об опасности использования ИИ в техноавторитарных целях, но Вашингтон не возглавил ни одной новой устойчивой коалиции для создания демократических альтернатив. Нынешняя политика представляет собой компиляцию разрозненных мероприятий, связанных с ИИ, осуществляемых федеральным правительством. Нигде нельзя найти стратегию в сочетании с организацией и ресурсами, чтобы выиграть соревнование ИИ и сохранить лидерство ИИ Соединённых Штатов.

Правительство должно будет организовывать политику поощрения инноваций; защищать отрасли и секторы, имеющие решающее значение для национальной безопасности; набирать и обучать талантливых специалистов; стимулировать внутренние исследования, разработки и производство по целому ряду технологий, считающихся необходимыми для национальной безопасности и экономического процветания; и создавать коалиции союзников и партнёров для поддержки демократических норм.

Некоторые элементы национальной стратегии должны быть скоординированы и воспроизведены на государственном уровне с помощью конкретных государственных стратегий поддержки исследований ИИ, торговли и образования.

Это потребует сложной последовательности действий по поощрению и защите, направленных на минимизацию издержек и рисков карательных мер; обеспечение взаимоукрепляющих программ фундаментальных и прикладных исследований; координацию подходов с международными партнёрами; и согласование приоритетов исполнительной власти с законодательными полномочиями. Также это потребует выявления технологических тенденций и оценки относительных преимуществ Соединённых Штатов и их конкурентов.

Кроме этого потребуется, прежде всего, сильное и последовательное руководство Белого дома.

Дело за руководством Белого дома.

Правительству потребуется центр силы, способный оказывать гравитационное воздействие на внутреннюю экономическую политику, национальную безопасность и научно - техническую политику. Сегодня у нас нет такой организации. Несколько отдельных органов Исполнительной власти Президента (EOP) обладают определённой ответственностью

и способностью выполнять основные организационные требования: Совет национальной безопасности (NSC),Управление научно-технической политики (OSTP) и связанный с ним Национальный научно-технический совет (NSTC) и Национальный экономический совет (NEC).

Совет по внутренней политике (DPC) также имеет важнейшие связанные с этим обязанности и аналогичный мандат с руководством в области иммиграционной политики, политики в области образования, и регулятивная политика.

Ещё один орган Управление по вопросам управления и бюджета (ОМБ) осуществляет надзор за соответствующими бюджетами и усилиями по проведению государственных реформ.

В отсутствие всеобъемлющей структуры Президент и вице-президент должны выявлять, выносить решения и согласовывать позиции, возникающие в результате параллельных межведомственных процессов, оставляя бесконечное пространство для оводов, чтобы заполнить пробелы и повлиять на Президента.

Президент нуждается в инструменте, который поможет принять решение и провести новую технологическую стратегию через необходимые, но недостаточные существующие советы и в остальную часть правительства.

Белый дом должен:

«Правительству потребуется центр власти, который сможет оказывать гравитационное воздействие на внутреннюю экономическую политику, национальную безопасность и научно-техническую политику. Сегодня у нас нет такой организации.»

Создать Совет по конкурентоспособности технологий. Соединённые Штаты должны укрепить исполнительное руководство в области технологической политики в Белом доме, предоставив возможность одному субъекту осуществлять всеобъемлющую технологическую стратегию.

Комиссия предлагает создать новый Совет по конкурентоспособности технологий (TCC), который будет включать в себя такое же объединение лидеров EOP и секретарей Кабинета министров, как и другие форумы Белого дома для созыва межведомственного совещания, и будет возглавляться вице-президентом с недавно назначенным помощником президента по конкурентоспособности технологий, выступающим в качестве повседневного лидера. TCC обеспечит заполнение пробелов между обязанностями NEC, OSTP и NSC и их увязку с OMB. Он не заменит НСК, НЭК или возглавляемые ОСТП структуры НСТК, но обеспечит форум для согласования конкурирующих приоритетов в области безопасности, экономики и науки и поднимет технологическую политику и проблемы с технического уровня на стратегический.

Для координации работы совета необходимо создать нового Директора-помощника Президента по вопросам конкурентоспособности технологий, ответственного за обеспечение того, чтобы политика, касающаяся новых технологий, получала достаточное внимание на уровне Президента.

Разработать Национальную технологическую стратегию. ТСС должна создать Национальную технологическую стратегию, основанную на тех элементах, которые мы здесь представляем, которые могут направлять политику США во всех ключевых новых технологиях, начиная с ИИ.

Цель Национальной технологической стратегии должна заключаться в обеспечении долгосрочного общего лидерства США в области технологий, особенно новых технологий, имеющих решающее значение для национальной безопасности и конкурентоспособности.

Стратегия должна взвешивать сложные компромиссы между конкурирующими политическими интересами и приоритетами, выявлять критические технологии, где конкуренты стремились соответствовать или обогнать лидерство США, и способствовать комплексному политическому подходу к новым технологиям.

В качестве отправной точки стратегия должна опираться на следующие основные принципы:

1) победа в конкурсе талантов ИИ;

2) продвижение американских инноваций ИИ;

3) защита преимуществ ИИ США;

4) лидерство в благоприятном международном порядке ИИ.

Установить всеобъемлющий научно-технический диалог между США и Китаем на высоком уровне. Соединённые Штаты должны наладить регулярный дипломатический диалог на высоком уровне с Китаем, который принесёт пользу американскому народу, сохранит верность нашим союзникам и заставит Китай соблюдать международные нормы.

Диалог должен быть сосредоточен на проблемах, связанных с новыми технологиями, включая ИИ, биотехнологии и другие технологии, согласованные обеими сторонами. Диалог должен иметь две всеобъемлющие цели:

• Определить целевые области сотрудничества в области новых технологий для решения глобальных проблем, таких как изменение климата и оказание помощи в случае стихийных бедствий;

• Обеспечить форум для обсуждения отдельных проблем, связанных с конкретным использованием новых технологий, при построении отношений и налаживании процессов между двумя странами.

Конкурс талантов

Победа в конкурсе талантов ИИ;

NDEA II С акцентом на цифровые навыки;

Привлекайте и удерживайте самых ярких людей в мире.

Соединённые Штаты находятся в глобальной конкуренции за редкие таланты в области искусственного интеллекта. Комиссия очень обеспокоена текущими тенденциями в области талантов.

Число отечественных студентов, участвующих в программах докторантуры по ИИ, не увеличилось с 1990 года, а конкуренция за иностранных студентов ускорилась, поставив под угрозу способность Соединённых Штатов удерживать иностранных студентов.

Впервые в нашей жизни Соединённые Штаты рискуют проиграть конкуренцию за таланты на научных рубежах. Культивирование большего числа потенциальных талантов внутри страны и привлечение и удержание большего числа существующих талантов из других стран-это единственные два варианта сохранения лидерства США.

«Впервые в нашей жизни Соединённые Штаты рискуют проиграть конкуренцию за таланты на научных рубежах.»

Конкуренты и союзники признают реализацию стратегий талантов ИИ. В период с 2000 по 2014 год университетская система Китая увеличила число выпускников в области науки, техники, инженерии и математики (STEM) на

360%, произведя 1,7 миллиона только в 2014 году. Число выпускников STEM в университетской системе Соединённых Штатов выросло на 54% за тот же период времени, и многие из них были иностранными студентами. Китайские исследователи в настоящее время представляют примерно 29% ведущих талантов в области глубокого обучения в мире. Китай и другие государства также предприняли шаги по привлечению международных талантов с помощью гибкой иммиграционной политики и стимулов для технических талантов.

Соединённым Штатам необходимо инвестировать во все трубопроводы талантов ИИ, чтобы оставаться на переднем крае ИИ сейчас и в будущем. Пассивная стратегия не сработает перед лицом конкуренции талантов ИИ.

Чтобы добиться доминирования в ИИ, США необходимо обучить четыре архетипа, которые будут продвигать ИИ в Америке: исследователей, разработчиков, конечных пользователей и информированных потребителей.

Инженеры-исследователи ИИ будут сосредоточены на Исследованиях и разработках технологий, которые позволяют и продвигают полу – и полностью автономные системы. Они служат экспертами по алгоритмам, обладающими современными знаниями в области современных исследований ИИ, и могут участвовать в зарождении идей и управлять циклами разработки от исследований до тестирования прототипов для крупного проекта или компонента крупного проекта.

Они будут отвечать за очистку данных, извлечение и отбор признаков, а также анализ; обучение и настройку моделей; партнёрские отношения с экспертами по знаниям предметной области и конечными пользователями; и обнаружение местных возможностей для использования.

Разработчики требуют меньше подготовки и образования, чем эксперты по ИИ, и будут иметь подготовку, образование и/или опыт, который примерно эквивалентен степени младшего специалиста или бакалавра; и это включает в себя соответствующую этику и смягчение предвзятости при обработке данных и обучении моделям.

Их ежедневный бизнес будет дополнен/включён ИИ. Использование ИИ будет сильно напоминать использование имеющегося в настоящее время программного обеспечения в том смысле, что оно потребует определённой системной подготовки, но, за исключением некоторых должностей, которые управляют данными, практически не будет иметь специальных знаний ИИ.

Информированные потребители

Эта группа людей нуждается в способности сделать лучший потребительский выбор при покупке технологии и понять важность своих действий на рынке.

Перспектива и пределы расширения.

Инвестиции в STEM-образование являются необходимой частью повышения американской национальной мощи и укрепления национальной безопасности. Соединённые Штаты в целом занимают хорошие позиции по международным показателям талантов из-за нашей способности привлекать международные таланты, несмотря на нашу неравномерную систему образования от детского сада до 12-го класса (К-12).

Крайне важно, чтобы Соединённые Штаты инвестировали значительные средства в STEM-образование как двигатель роста талантов в области искусственного интеллекта в Америке.

Однако одних инвестиций в STEM - образование будет недостаточно для того, чтобы Соединённые Штаты выиграли международный конкурс талантов в области искусственного интеллекта и STEM. Китай производит большое количество компьютерных учёных, инженеров и других выпускников STEM. В обозримом будущем система образования STEM Соединённых Штатов не обладает ни потенциалом, ни качеством для производства достаточного количества талантов STEM или AI для обеспечения рынков Соединённых Штатов или предприятий национальной безопасности.

Чтобы конкурировать, Соединённые Штаты должны реформировать свою систему образования, чтобы выпускать как более качественные, так и более качественные выпускники.

Рекомендация

Принять Закон об образовании в области национальной обороны II. Движимый страхом, что Америка отстала в образовании и инновациях после того, как СОВЕТЫ запустили Спутник в 1957 году, Конгресс принял Закон об образовании в области национальной обороны (NDEA) в следующем году. NDEA пропагандировал важность науки, математики и иностранных языков для студентов, разрешив более 1 миллиарда долларов на сокращение студенческих кредитов, финансирование образования на всех уровнях и финансирование аспирантур.

Многие студенты смогли поступить в колледж из-за этого закона.

В 1960 году колледж посещали 3,6 миллиона студентов; к 1970 году их было 7,5 млн.10 Этот акт помог Америке выиграть Космическую гонку, способствовал развитию микроэлектронной промышленности, ускорил способность США к инновациям и, в конечном счёте, сыграл важную роль в победе Америки в холодной войне.

Комиссия считает, что настало время для второго NDEA, который отражает первый закон, но с важными различиями. NDEA II будет сосредоточена на финансировании студентов, приобретающих цифровые навыки, такие как математика, информатика, информатика, наука о данных и статистика. NDA II должна включать в себя программы образования K-12 и рескиллинга, которые устраняют недостатки по всему спектру американской системы образования, целенаправленно ориентируясь на недостаточно обеспеченные ресурсами школьные округа. Комиссия также рекомендует инвестировать в программы STEM университетского уровня с 25 000 стипендиями для студентов, 5 000 аспирантов и 500 стипендиями для аспирантов.

Стипендии для студентов должны включать в себя зачётные часы в общественных колледжах, чтобы обеспечить большему числу американцев доступ к доступному STEM-образованию. В конечном счёте, цель NDEA II

заключается в расширении цифрового кадрового резерва путём стимулирования программ для недопредставленных американцев.

«Комиссия считает, что настало время для второго НДЭА ...»

Укрепляйте таланты ИИ с помощью иммиграции. Иммиграционная реформа - это императив национальной безопасности. Страны, которые могут успешно привлекать и удерживать высококвалифицированных специалистов, получают стратегические и экономические преимущества перед конкурентами.

Преимущества человеческого капитала особенно значительны в области ИИ, где спрос на таланты намного превышает предложение. Высококвалифицированные иммигранты ускоряют американские инновации, улучшают предпринимательство и создают рабочие места.

Соединённые Штаты получают гораздо больше выгод от иммиграции высококвалифицированных иностранных рабочих, чем другие страны.

В 2013 году в Соединённых Штатах было в 15 раз больше изобретателей-иммигрантов, чем американских изобретателей, живущих за границей.

Напротив, Канада, Германия и Великобритания поддерживают чистый отрицательный уровень иммиграции изобретателей.14

По сравнению с другими преимуществами США в конкурентной борьбе за ИИ такими как финансовые ресурсы или аппаратные возможности — это иммиграционное преимущество труднее воспроизвести другим странам.

«Страны, которые могут успешно привлекать и удерживать высококвалифицированных специалистов, получают стратегические и экономические преимущества перед конкурентами.»

К сожалению, иностранные студенты в США все чаще предпочитают учиться в других странах или возвращаться домой. Одной из причин является растущее отставание в подаче петиций по грин-картам.

Индийским иммигрантам приходится особенно долго ждать. Многие из них проведут десятилетия на стеснительных рабочих визах в ожидании получения своих грин-карт, препятствуя как способности технологического сектора набирать таланты, так и качеству жизни индийских иммигрантов.

В то же время другие страны наращивают свои усилия по привлечению и удержанию талантов в области искусственного интеллекта, в том числе иммигрантов из Кремниевой долины.17

«Ограничения наносят ущерб инновациям и экономическому росту США и только помогают нашим конкурентам, позволяя их человеческому капиталу расти. Они также стимулируют американские технологические компании двигаться туда, где живут таланты, будь то прямо через наши границы или за рубежом.»

Хотя иммиграция приносит пользу Соединённым Штатам, политики также должны учитывать угрозу нежелательной передачи технологий.

Однако ограничение иммиграции-слишком тупой инструмент для решения этой проблемы.18 Ограничения наносят ущерб инновациям и экономическому росту США и помогают нашим конкурентам, позволяя их человеческому капиталу расти. Они также стимулируют американские технологические компании двигаться туда, где живут таланты, будь то прямо через наши границы или за рубежом.

Передача технологий будет только ухудшаться, если значительные компоненты США технологический сектор переносит свои исследования и разработки в Китай или другие страны, которые более уязвимы для усилий по передаче технологий, чем Соединённые Штаты.20 Более эффективный стратегический подход мог бы сочетать действия по повышению способности Соединённых Штатов привлекать лучшие мировые таланты с целенаправленными усилиями по борьбе с векторами передачи технологий. NSCAI подробно рассматривает передачу технологий. Изменения в иммиграционной политике должны сопровождаться этими рекомендациями.

Иммиграционная политика также может замедлить прогресс Китая. Китайское правительство серьёзно относится к угрозе утечки мозгов, отмечая, что способность Соединённых Штатов привлекать и удерживать таланты Китая является препятствием для амбиций Коммунистической партии Китая (КПК).

Увеличение утечки мозгов из Китая создаст дилемму для КПК, которая будет вынуждена выбирать между потерей ещё большего человеческого капитала, дальнейшим замедлением экономического роста и угрозой их продвижению в области ИИ, или лишением китайских граждан возможности учиться и работать в Соединённых Штатах. В то же время Соединённые Штаты должны проявлять осторожность в отношении потенциальных негативных последствий для кадровых резервов в странах-партнёрах.

«Увеличение утечки мозгов из Китая создаст дилемму для КПК»

Расширьте сферу применения «экстраординарных» талантов, чтобы сделать визу O-1 более доступной и подчеркнуть талант ИИ. Временная рабочая виза Teo-1 предназначена для людей с экстраординарными способностями или достижениями. В настоящее время судьи определяют правомочность заявителя на основании субъективной оценки. Для науки и техники это в значительной степени соответствует академическим критериям, таким как публикации в крупных изданиях, и не очень хорошо подходит для людей, которые преуспевают в промышленности.

Внедряйте и рекламируйте правило международного предпринимателя. Правило международного предпринимателя (IER) позволяет американским службам гражданства и иммиграции (USCIS) предоставлять период разрешённого пребывания международным предпринимателям, которые демонстрируют, что «их пребывание в Соединённых Штатах принесёт значительную общественную пользу через их деловое предприятие».

USCIS также можно было бы поручить объявить, что она будет отдавать приоритет предпринимателям, работающим в высокоприоритетных областях STEM, таких как ИИ, или в областях, использующих ИИ для других применений, таких как сельское хозяйство. Способность предпринимателей привлекать инвесторов должна использоваться в качестве критерия отбора предпринимателей.

Расширьте и уточните переносимость рабочих мест для высококвалифицированных работников. Критерии для работников с H1B, O-1 и

другими временными рабочими визами для получения разрешений на работу на открытом рынке на годичный возобновляемый период слишком ограничены и неоднозначны. Изменения должны прояснить, когда высококвалифицированным не иммиграционным работникам разрешается менять работу или работодателей, повысить гибкость работы, когда работодатель либо отзывает своё ходатайство, либо выходит из бизнеса, а также повысить гибкость для работников H-1B, ищущих другую работу H-1B.

Вернуть грин-карты, потерянные из-за бюрократической ошибки. Федеральные агентства обычно выдают меньше грин-карт, чем им разрешено. По состоянию на 2009 год федеральное правительство не выдало более 326 000 грин-карт из-за совокупной бюрократической ошибки. Департаменты государственной и внутренней безопасности (DHS) должны опубликовать обновлённый отчёт о количестве грин-карт, потерянных из-за бюрократической ошибки. Используя имеющиеся полномочия, оба должны выдавать потерянные грин-карты заявителям, ожидающим своей очереди. Конгресс должен поддержать Государственные департаменты и Министерство внутренней безопасности, приняв закон о возвращении утерянных грин-карт.

Выдайте грин-карты студентам, получившим степень доктора философии STEM в аккредитованных американских университетах. Конгресс должен внести поправки в Закон об иммиграции и гражданстве, чтобы предоставить законное постоянное место жительства любому проверенному (не представляющему угрозы национальной безопасности) иностранному гражданину, который окончил аккредитованное высшее учебное заведение Соединённых Штатов с докторской степенью в области, связанной со STEM, в резидентной или смешанной резидентной и дистанционной программе и имеет предложение о работе в области, связанной с наукой, техникой, инженерией или математикой. Они не должны учитываться в качестве постоянных резидентских шапок.

Удвоить количество грин-карт, основанных на трудоустройстве. При нынешней системе грин-карт, основанных на трудоустройстве, крайне мало:

140 000 в год, из которых менее половины достаётся основному работнику. В результате этого многие высококвалифицированные работники не могут получить постоянное место жительства и не могут переводить работу или вести переговоры с работодателями так же эффективно, как домашняя прислуга. Это снижает привлекательность присоединения к американской рабочей силе. Чтобы сократить отставание высококвалифицированных работников, Соединённым Штатам следует удвоить число грин-карт, основанных на трудоустройстве, с акцентом на постоянное проживание в областях, связанных с STEM и ИИ.

Создайте визу предпринимателя. Иностранные докторанты с большей вероятностью, чем их родные сверстники, захотят основать компанию или стать сотрудником стартапа, но они с меньшей вероятностью пойдут по этому пути.27 Одной из причин являются ограничения визовой системы H-1B. Точно так же предприниматели-иммигранты, не имеющие капитала для использования маршрута EB-5 для постоянного проживания, вынуждены использовать другие визы, предназначенные для учёных и работников существующих компаний, а не для предпринимателей. Все эти проблемы делают Соединённые Штаты менее привлекательными для международных талантов и, возможно, столь же важными, уменьшите способность стартапов и других небольших компаний основного источника новых рабочих мест для американцев нанимать высококвалифицированных иммигрантов, которые, как было показано, повышают шансы на успех бизнеса. Конгресс должен создать визу предпринимателя для тех, кто предоставит «значительную общественную выгоду» Соединённым Штатам, если им разрешат остаться в стране на ограниченный испытательный срок для развития своих компаний. Эта виза должна служить альтернативой визам, спонсируемым сотрудниками, инвесторами или студентами, и вместо этого должна быть нацелена на перспективных потенциальных основателей.

Создайте новую и разрушительную технологическую визу. Национальный научный фонд (NSF) должен выявлять критические новые

технологии каждые три года. Затем DHS позволит студентам, исследователям, предпринимателям и технологам в соответствующих областях подавать заявки на получение новых и прорывных технологических виз. Это обеспечило бы столь необходимые исследования и разработки в области талантов и укрепило бы нашу экономику.

Ускорение инноваций в области ИИ

Лидерство в инновациях ИИ;

Масштабирование и Координация Федерального финансирования исследований и разработок в области ИИ;

Расширение Доступа через Национальную Инфраструктуру Исследований И Разработок В Области ИИ;

Укрепление Государственно-частного партнёрства;

Решите Самые большие проблемы человечества.

Чтобы оставаться мировым лидером в области искусственного интеллекта (ИИ), правительство США должно подтвердить свою приверженность инвестированию в национальную силу Америки-инновации.

Это потребует значительных новых инвестиций в AIR&D и создания национальной исследовательской инфраструктуры ИИ, которая демократизирует доступ к ресурсам, питающим ИИ.

Члены Конгресса должны смириться с тем, что в ближайшие несколько лет потребуются десятки миллиардов долларов. Отдача от этих инвестиций изменит американскую экономику, общество и национальную безопасность.

Отсутствие национальной срочности опасно в то время, когда в нашей экосистеме ИИ появились глубинные слабости, которые мешают инновациям, и когда это рассматривается на фоне государственного прогресса ИИ в Китае. Развитие ИИ в Соединённых Штатах сосредоточено в меньшем количестве

организаций в меньшем количестве географических регионов, преследующих меньшие исследовательские пути. Коммерческие программы диктуют будущее ИИ и в значительной степени концентрируются в одной дисциплине: машинном обучении (мл). Несмотря на многообещающие шаги, государственное финансирование отстаёт от трансформационного потенциала этой области, ограничивая её способность формировать исследования в интересах общественного блага и поддерживать прогресс по целому ряду дисциплин ИИ. В результате инновационная среда ИИ опирается на сужающийся фундамент.

«Отсутствие национальной срочности опасно в то время, когда в нашей экосистеме ИИ появились основные слабости, которые мешают инновациям, и когда это рассматривается на фоне государственного прогресса ИИ в Китае.»

Эти тенденции к консолидации возникают в результате использования ресурсов. Снижение удельных затрат на облачные вычисления и доступность платформ с открытым исходным кодом снизили барьеры для доступа к базовым мл.

Однако те же самые условия позволили создать сложные модели, требующие обширных обучающих данных, часто хранящихся в частных контролируемых наборах данных или графиках знаний, огромной вычислительной мощности и значительной аппаратной и программной инженерии.

Эти предпосылки в настоящее время определяют передний край исследований ИИ и эффективно ограничивают число американских исследователей, способных внести свой вклад в эту область и решить трудные задачи, которые могли бы открыть новые границы ИИ.

Изобретательность, а не доступ, должна быть ключом к инновациям ИИ в Америке.

Консолидация индустрии ИИ угрожает технологической конкурентоспособности США пятью способами:

• Утечка мозгов. Утечка мозгов из академических институтов в частный сектор угрожает опустошить основы преимущества Соединённых Штатов в фундаментальных исследованиях ИИ: их университеты. Федеральное финансирование, которое не шло в ногу с ростом отрасли, привело к низким показателям успеха заявок на гранты и увеличило время, затрачиваемое на бюрократическую работу по поиску и завершению предложений. Однако академических экспертов и их студентов не просто заманивают в большие технологии обещанием меньшего количества бюрократии и более высоких финансовых стимулов.

Все чаще частный сектор становится лучшим местом для проведения передовых исследований с доступом к лучшим вычислительным и информационным ресурсам. Результатом является ослабление преподавательской базы для следующего поколения лидеров ИИ в промышленности и академических кругах и сужение общей программы исследований ИИ.

Вычисления, необходимые для обучения Крупнейших моделей глубокого обучения (2012-2017)

«Петафлоп/с-день» – это мера вычислений, которая состоит из выполнения 10^15 операций с плавающей запятой в секунду в течение одного дня.

GPT-3 и более поздние модели здесь не представлены, потому что они слишком велики, чтобы поместиться в этом масштабе.

• Разнообразие. Растущий разрыв между «имущими» и «неимущими» в ИИ усугубит хорошо задокументированное отсутствие разнообразия в этой области, ограничивая коллективную способность этой области создавать справедливые, инклюзивные системы.

• Исследовательская Направленность. Американские технологические фирмы подотчётно своим акционерам и логично не будут инвестировать в области, имеющие значение для национальной безопасности, или делать

неопределённые ставки на фундаментальные исследования, которые не несут коммерческой или экономической выгоды для компании.

Хотя инвестиции, ориентированные на отдачу, могут привести к приложениям, которые способствуют общественному благу или приносят пользу работе правительства, существуют пробелы.

мл и лежащие в его основе алгоритмы находились именно в таком положении два десятилетия назад казалось бы, без коммерческих перспектив только для того, чтобы быть поддержанными федеральными исследовательскими долларами, пока вычислительная мощность и избыток данных не трансформировали дисциплину.

Недавнее исследование показало, что 82% алгоритмов, используемых сегодня, исходят от финансируемых из федерального бюджета некоммерческих организаций и университетов, по сравнению с 18%, которые исходят от частных компаний.10

• Конкуренция. Рост стоимости разработки передовых моделей мл и высокая вероятность приобретения ведущими технологическими компаниями означает, что стартапы ИИ имеют сужающиеся пути роста в Соединённых Штатах.11 Отсутствие конкуренции подрывает способность отрасли к инновациям и глобальной конкуренции в области исследований и разработок ИИ.

• Региональная дивергенция. Кластеризация технологических фирм в таких регионах, как Кремниевая долина, стимулирует инновации, ускоряя обмен знаниями и обостряя внутреннее соперничество. Однако эта тенденция принесла пользу некоторым регионам и демографическим показателям в большей степени, чем другим. Более 90% рабочих мест в инновационном секторе США было создано всего в пяти крупных прибрежных городах в период с 2005 по 2017 год. Это расхождение концентрирует выгоды от технологического прогресса всего в нескольких регионах и упускает скрытый инновационный потенциал в остальной части страны.

Федеральное правительство несёт ответственность за то, чтобы обратить вспять эти тенденции. Она должна вмешиваться и усиливаться, чтобы обеспечить стратегическое направление и устойчивые ресурсы, как финансирующий и потребитель технологии. Она должна сломать стереотип стандартного финансирования научных исследований. Результаты технологических инноваций, которые приносят наибольшую ценность при переводе в полевые решения, обусловлены вкладом многих секторов и культурой принятия рисков.

Статус-кво федеральных агентств и исследовательских организаций недостаточен для того, чтобы делать такие большие ставки и продвигать перспективные технологические концепции из лаборатории в поле.

Пассивный национальный подход, который слишком сильно полагается на частный сектор для стимулирования инноваций и определения исследовательских программ и который предполагает, что коммерческие инновации могут просто «закручиваться», чтобы стать правительственными приложениями, -не выиграет эту стратегическую конкуренцию и не сможет полностью использовать трансформационный потенциал ИИ. Соединённые Штаты через руководство правительства в партнёрстве с промышленностью и научными кругами должны увеличить разнообразие, конкурентоспособность и доступность своей инновационной среды ИИ. Это начинается с существенного вливания новых долларов на НИОКР.

«Соединённые Штаты через руководство правительства в партнёрстве с промышленностью и академическими кругами должны увеличить разнообразие, конкурентоспособность и доступность своей инновационной среды ИИ.»

Масштабирование и координация федерального финансирования исследований и разработок в области ИИ. Смелый, комплексный толчок к долгосрочным инвестициям в AIR&D будет способствовать общенациональным инновациям в области искусственного интеллекта и стимулировать прорывы. Вливание устойчивых ресурсов, управляемых

всеобъемлющей стратегией и распределяемых через разнообразные механизмы, позволит американским исследователям раздвинуть границы этой области, поддерживая широкий спектр подходов к ИИ и новые приложения ИИ в других областях. В частности, Соединённые Штаты должны:

• Создать Национальный технологический фонд (НТФ). Новая, независимая организация будет дополнять успешные существующие организации, такие как NSF и DARPA, предоставляя средства для более агрессивного продвижения науки в инженерию. НТФ будет стимулировать технологический прогресс на национальном уровне, сосредоточив внимание на создании ценности на промежуточных уровнях технической зрелости, приоритизации концепций, основанных на использовании, создании инфраструктуры для экспериментов и испытаний и поддержке коммерциализации успешных результатов. Для этого требуется организация, которая структурирована так, чтобы принимать более высокие уровни риска и иметь возможность делать большие ставки на инновационные идеи и людей.

• Увеличить федеральное финансирование исследований и разработок в области ИИ, не связанных с обороной, в два раза в год, чтобы достичь 32 миллиардов долларов в год к 2026 финансовому году. Это позволило бы довести расходы на ИИ до уровня, близкого к федеральным расходам на биомедицинские исследования. В целом правительство должно тратить не менее 1% ВВП на НИОКР, чтобы укрепить инновационную базу в научных областях. Дополнительное финансирование должно укрепить фундаментальные и прикладные исследования, расширить программы стипендий, поддержать исследовательскую инфраструктуру и охватить несколько агентств с акцентом на:

Национальный технологический фонд (предлагается)

Министерство энергетики

Национальный научный фонд

Национальные институты здравоохранения

Национальный институт стандартов и технологий

Национальное управление по аэронавтике и исследованию космического пространства

DHS - Министерство внутренней безопасности DOE - Министерство энергетики DOI - Департамент внутренних дел DOT - Департамент транспорта FDA - Управление по контролю за продуктами и лекарствами НАСА - Национальное управление по аэронавтике и исследованию космического пространства NIH - Национальные институты здравоохранения NIJ - Национальный институт юстиции	NIST - Национальный институт стандартов и технологий NOAA - Национальное управление океанических и атмосферных исследований NSF - Национальный научный фонд Казначейство - Казначейство/Сеть по борьбе с финансовыми преступлениями USDA - Министерство сельского хозяйства США VA - Департамент по делам ветеранов

Источник: Программа исследований и разработок в области сетевых и информационных технологий, Дополнение к Бюджету Президента на 2021 финансовый год, Национальный совет по науке и технологиям (14 августа 2020 года), https://www.nitrd.gov/pubs/FY 2021-NITRD-Дополнение.pdf.

• Определение приоритетов финансирования ключевых направлений НИОКР в области ИИ. Усиленное федеральное финансирование должно уделять приоритетное внимание инвестициям в НИОКР ИИ в областях, имеющих решающее значение для развития технологий, которые будут лежать в основе будущей национальной безопасности и экономической стабильности, поддерживая области, которые могут не получить значительных инвестиций частного сектора. Координируемые в рамках недавно созданной Национальной инициативы по

ИИ18 инвестиции должны отражать портфельный подход, ориентированный на развитие фундаментальной науки, решение конкретных проблемных задач и содействие прорывам в коммерциализации.

Приоритетные направления инвестиций в исследования ИИ.

Новые направления машинного обучения (мл)	Тестирование и оценка, верификация и валидация (TEVV)	Надёжный и устойчивый ИИ	Сложные мультиагентные сценарии
Далее следуют нетрадиционные подходы к контролируемому ОД в неконтролируемой или полуконтролируемой манере, а также перенос обучения с одной задачи или предметной области на другую.	Развивайте лучшее понимание того, как характеризовать производительность системы ИИ, включая усовершенствованные методы прогнозирования поведения системы ИИ в контекстах системных систем и новых средах.	Развивайте методы, которые могут преодолеть неблагоприятные условия, включая различные классы состязательных атак, и продвигайте подходы, которые позволяют оценить типы и уровни уязвимости, иммунитета и справедливости	Развивайте понимание взаимодействующих когорт систем искусственного интеллекта, включая исследования конкурентных уязвимостей и смягчающих воздействий, а также применение теории игр к разнообразным и сложным сценариям.

		.	
Интегрированный ИИ, моделирование, имитация и дизайн			Расширенное понимание сцены
Развивайте использование симуляций в качестве источников данных и сценариев для обучения и тестирования систем ИИ, а также используйте ИИ в качестве генеративного двигателя проектирования в научных открытиях и инженерии.			Эволюционируйте перцептивные модели, чтобы включить многоисточниковую и мультимодальную информацию для поддержки расширенной практической осведомлённости и понимания в различных сложных, динамичных средах и сценариях.
Сохранение личной конфиденциальности			Оценка рисков системы ИИ
Обеспечение защиты	К более общему искусственному		Расширенные возможности

конфиденциальности при использовании данных для разработки и эксплуатации ИИ с помощью достижений в области методов и технологий анонимности, таких как многопартийное федеративное обучение.	интеллекту Исследуйте проблемы и тайны человеческого интеллекта, включая способность учиться без присмотра, накапливать и применять здравый смысл, строить причинные модели, осуществлять самосознание и обобщать знания.		поддержки оценки рисков, включая стандартные методы и метрики для оценки степени проверяемости, прослеживаемости, интерпретируемости, объяснимости и надёжности.
Улучшенное взаимодействие человека и ИИ и объединение в команду			Автономные системы ИИ
Развивайте понимание комплементарности человека и ИИ, методов расширения человеческого мышления, плавных передач в системах со			Повышение способности системы самостоятельно или с минимальным контролем со стороны человека-оператора достигать

смешанной инициативой и восприятия технологий ИИ человеческих намерений и коммуникаций.			поставленных целей в сложных и непредсказуемых условиях.

• Утроить число Национальных исследовательских институтов ИИ. Правительство должно утроить нынешнее число финансируемых из федерального бюджета национальных научно-исследовательских институтов ИИ по целому ряду регионов и областей исследований. Это расширит возможности обучения и исследований для студентов и преподавателей, национальных лабораторных исследователей и некоммерческих исследовательских организаций.

• Инвестируйте в таланты, которые преобразят сферу. Параллельно NSF или предлагаемый NTF должны инвестировать в ведущих исследователей ИИ и междисциплинарные команды, запуская грантовые премии, которые делают большие ставки на людей и нестандартные идеи, которые могут привести к неожиданным прорывам.

«Демократизированный доступ к вычислительным средам, данным и средствам тестирования предоставит исследователям за пределами ведущих игроков отрасли и элитных университетов возможность добиваться прогресса на переднем крае ИИ.»

Расширьте доступ к ресурсам ИИ через Национальную исследовательскую инфраструктуру ИИ. Демократизированный доступ к вычислительным средам, данным и средствам тестирования предоставит исследователям, выходящим за рамки ведущих игроков отрасли и элитных университетов, возможность добиваться прогресса на переднем крае ИИ. Это укрепит фундамент американских инноваций в области ИИ, поддерживая более

справедливый рост отрасли, расширяя опыт ИИ по всей стране и применяя ИИ в более широком спектре областей. Эта национальная инфраструктура должна иметь пять основных элементов:

• Национальный исследовательский ресурс по ИИ (NAIRR). Чтобы преодолеть «разрыв в вычислениях», NAIRR предоставит проверенным исследователям и студентам субсидируемый доступ к масштабируемым вычислительным ресурсам, расположенным совместно с готовыми к ИИ правительственными и неправительственными наборами данных, образовательными инструментами и поддержкой пользователей. Он должен быть создан как государственно-частное партнёрство с использованием федерации облачных платформ.

• Набор предметно-ориентированных испытательных стендов для исследований и разработок в области ИИ. Спонсируемые различными федеральными агентствами, они обеспечат доступные средства, установят стандарты бенчмаркинга и создадут сообщества открытий вокруг областей применения ИИ, отвечающих общественным интересам.

• Крупномасштабные, открытые данные обучения. Это должно включать в себя кураторство, размещение и обслуживание сложных наборов данных; стимулы для частного сектора и академических кругов обмениваться наборами данных; а также финансирование групп инженеров и учёных по обработке данных для разблокирования открытых данных, находящихся в настоящее время в распоряжении правительства для использования исследовательским сообществом ИИ.

• Открытая сеть знаний. Координируемый Управлением по научно - технической политике, такой ресурс позволил бы использовать сконструированные и организованные мировые знания для разработки систем искусственного интеллекта, которые функционировали бы эффективно и действенно.

• Многосторонний Научно-исследовательский институт ИИ. Развивать совместные исследования и разработки с исследователями из ключевых союзников и партнёров (подробнее описано в главе 15 настоящего доклада).

Национальная Исследовательская инфраструктура ИИ.

Рекомендация

Лидерство США в таких технологиях, как искусственный интеллект, зависит от более тесного сотрудничества между государственным и частным секторами и общего чувства ответственности за глобальную конкурентоспособность США. Для содействия инновациям и ускорения роста глобально конкурентоспособных фирм в стратегических развивающихся секторах правительство должно:

• Создание рынков для ИИ и других стратегических технологий. Применение ИИ в государственных учреждениях может сэкономить деньги налогоплательщиков и повысить качество государственных услуг. Некоторые заявки могут быть приняты непосредственно из частного сектора, в то время как другие являются уникальными для правительственной миссии. Ускоряя внедрение ИИ в федеральных ведомствах, правительство может стимулировать дополнительные коммерческие инвестиции в приложения ИИ, которые приносят пользу национальной безопасности и общественному благу.

• Формирование сети региональных инновационных кластеров, ориентированных на стратегические новые технологии. Правительство должно определить региональные инновационные кластеры, ориентированные на стратегические новые технологии, такие как ИИ, для стимулирования роста малых компаний в секторах, имеющих решающее значение для общей конкурентоспособности США. Созданные на конкурсной основе, кластеры будут предлагать участникам из промышленности и других отраслей: Региональные инновационные кластеры США, налоговые льготы, исследовательские гранты и доступ к федеральным ресурсам НИОКР.

*Сила кластера – то процент торгуемой занятости в регионе с высокой специализацией занятости. Это один из многих важных факторов, которые необходимо учитывать при выборе мест размещения региональных инновационных кластеров.

Источник изображения: Проект кластерного картографирования США, Институт стратегии и конкурентоспособности Гарвардской школы бизнеса. Источник данных: Бюро переписи населения США.

Частный сектор должен:

• Частное финансирование консорциума по конкурентоспособности ИИ. Частные фирмы должны создать некоммерческую организацию с финансированием в размере 1 миллиарда долларов в течение пяти лет для расширения возможностей исследований ИИ и поддержки навыков ИИ и образования. Эта организация, финансируемая за счёт пожертвований, будет сосредоточена на стимулировании экономических возможностей за счёт ресурсов для исследований ИИ и обучения навыкам ИИ. Такие расходы на корпоративную социальную ответственность, направленные на развитие ИИ-образования и предпринимательства, помогут преодолеть разрыв между цифровыми «имущими» и «неимущими.»

Решите некоторые из самых больших проблем человечества.

Сосредоточившись на решении реальных человеческих проблем, влияющих на жизнь миллионов людей, мы можем создать новый смысл существования трёхстороннего альянса правительства, научных кругов и промышленности ...»

Интеллектуальная собственность

Политика в области интеллектуальной собственности является приоритетом национальной безопасности

Издать Исполнительный указ об ИС для ИИ и новых технологий.

Разработать план реформирования и установления Политики и режимов в области ИС.	Оцените «Соображения ИС.»
Предложите Исполнительные и Законодательные действия.	Интегрироваться в Стратегии национальной безопасности, экономической и технологической конкурентоспособности.

Китай одновременно использует и использует политику в области интеллектуальной собственности (ИС) в качестве важнейшего инструмента в рамках своих национальных стратегий развития новых технологий. Соединённые Штаты также не смогли признать важность ИС в обеспечении своей национальной безопасности, экономических интересов и технологической конкурентоспособности. США не разработали всеобъемлющей политики в области ИС для стимулирования инвестиций и защиты создания искусственного интеллекта (ИИ) и других новых технологий.

Последствия этой политики недействительны, что включает в себя правовую неопределённость, созданную нынешними США. доктрина патентного права и патентоспособности, отсутствие эффективного ответа на внутренние и геополитические стратегии Китая, ориентированные на его институты ИС, и отсутствие эффективной политики защиты данных, это то, что США могут потерять свои главные позиции в мировом лидерстве в области ИС. В то же время, укрепляя свои режимы ИС, Китай готов «заполнить пустоту», оставленную ослабленной защитой ИС США, особенно в отношении патентов, поскольку США она утратила своё «сравнительное преимущество в обеспечении стабильных и эффективных прав собственности на новые технологические инновации».

Эта резкая асимметрия политики имеет множество существенных внутренних и международных последствий для США:

Во-первых, американские суды строго ограничили, какие типы компьютерных и биотехнологических изобретений могут быть защищены в соответствии с патентным законодательством США. Критические ИИ и связанные с биотехнологией изобретения были лишены патентной защиты с 2010 года. Сталкиваясь с неопределённостью в получении и сохранении патентной защиты, изобретатели преследуют защиту коммерческой тайны. Коммерческая тайна не способствует быстрому развитию рынков инноваций, поскольку коммерческая тайна, в отличие от патентов, не способствует доступу технических знаний в общественное достояние. Хотя эти последствия могут быть не немедленными, долгосрочные последствия для ИИ и других новых технологических разработок и конкурентоспособности вызывают озабоченность.9

Во-вторых, Китай выполнил свою стратегическую политическую задачу по увеличению количества своих патентных заявок и выданных патентов, создав представление о том, что он «выиграл» инновационную гонку. В 2019 году общее количество патентных заявок на «изобретения», поданных в Китайское национальное управление интеллектуальной собственности (CNIPA), было примерно в три раза больше, чем заявок на патенты на полезные изобретения, поданных в США. Бюро по патентам и товарным знакам (USPTO). Китай также лидирует в мире по международным патентным заявкам в рамках системы Договора о патентной кооперации (PCT) Всемирной организации интеллектуальной собственности (ВОИС). Критически важно отметить, что в настоящее время Китай часто называют нынешним лидером по подаче внутренних патентных заявок на изобретения в области искусственного интеллекта. Во всем мире число патентных заявок на ИИ, поступающих из Китая, превышает число заявок, поступающих из Соединённых Штатов, особенно в последние годы.

«США не разработали всеобъемлющей политики в области ИС для стимулирования инвестиций и защиты создания ИИ и других новых

технологий. Следствие этой политики ничтожно ... разве что США могут потерять свои главные позиции в мировом лидерстве ИС.»

Тенденции развития ИС в Китае.

Национальные режимы ИС Китая для ИИ и новых технологий Национальный 13-й пятилетний план развития Стратегических развивающихся отраслей формулирует связанные с ИС цели для новых технологий: Пересмотр Патентного законодательства и авторского права Укрепление защиты прав ИС через центры быстрой защиты прав Разработка стратегических планов продвижения прав ИС новых технологий Улучшение зарубежных прав ИС и поддержка компаний, участвующих в зарубежных слияниях и поглощениях	Патентные заявки стимулируются: Патентные субсидии Награды за выданные патенты Патентные квоты устанавливаются провинциальными или муниципальными органами власти Преференциальный режим в процессах государственных закупок для компаний с китайской интеллектуальной собственностью Патентная защита усиливается за счёт предварительных судебных запретов за нарушение патента, увеличения штрафных убытков за нарушение ИС (допускает пятикратный ущерб за умышленное нарушение) и специализированных судов по ИС с эффективным разрешением и низкими судебными издержками.

CSET Перевод Национального 13-го пятилетнего плана развития стратегических развивающихся отраслей промышленности Центрального

комитета Коммунистической партии Китая и Государственного Совета КНР (Опубликован 29 ноября 2016 г.) (перевод CSET от 9 декабря 2019 г.), https://cset.georgetown.edu/research/national-13thfive-year-plan-for-the-development-of-strategic-emerging-industries//; Эрик Уорнер, Патентование и инновации в Китае: стимулы, политика и результаты, RAND at 17-18 (Nov. 2014), https://apps.dtic.mil/dtic/tr/fulltext/u2/a619128.pdf; Товарные знаки и патенты в Китае: Влияние нерыночных факторов на тенденции подачи заявок и системы ИС, Бюро патентов и торговли США (январь 2021 г.), https://www.uspto.gov/sites/default/files/documents/USPTO-TrademarkPatentsInChina.pdf; Райан Дэвис, 4 вещи, которые нужно знать О Пересмотренном Патентном Законе Китая, Закон 360 (5 ноября 2020 Года), https://www.law360.com/articles/1326419/; Судья Тао Кайюань, Приверженность Китая укреплению судебной защиты ИС и созданию Светлого будущего для прав ИС, Журнал ВОИС (июнь 2019 г.), https://www.wipo.int/wipo_magazine/en/2019/03/article_0004.html.

Примечание: Самопровозглашённые номера патентов 5G standard-essential относятся к февралю 2020 года и представляют собой совокупную сумму от двух компаний, которые являются крупнейшими заявителями в каждой стране. Для Соединённых Штатов 2163 представляют собой 1293 заявки, поданные от Qualcomm, и 870-от Intel. Для Китая 5708 представляет собой 3147 поданных от Huawei и 2 561 поданных от ZTE. Это число также представляет собой стандартные основные патенты, поданные, а не количество выданных патентов. См. Jed John Ikoba, Huawei Подала Наибольшее количество патентов на 5G в мире по состоянию на февраль 2020 года - Отчёт Gizmochina (2 июня 2020 года), https://www. gizmochina.com/2020/06/02/huawei-has-the-most-5g-standard-essential-patents-globally/; Китай становится Ведущим Поставщиком международных патентов в 2019 году на фоне Устойчивого роста услуг ВОИС в области ИС, Договоров и финансов, Медиацентр ВОИС (7 апреля 2020 года), https://www.wipo.int/pressroom/en/articles/2020/article_0005.html Что касается

заявок национального патентного ведомства, то, по данным Национального управления интеллектуальной собственности Китая (CNIPA), «число полученных им патентных заявок на изобретения выросло более чем на 500 процентов в период с 2009 по 2019 год, с 241 000 до 1,4 миллиона (хотя, что интересно, с 2018 по 2019 год произошло снижение на 9 процентов). Для сравнения, количество патентных заявок в ВПТЗ США за тот же период выросло всего на 35% (с 456 000 до 621 000). Следовательно, в то время как в 2009 г. число патентных заявок превышает число китайских заявок почти в два раза, а к 2019 году это соотношение полностью изменилось. Большую часть роста китайского патентования можно отнести к заявкам, поданным отечественными заявителями. Из 1,4 миллиона заявок CNIPA в 2019 году внутренние источники подали почти 90 процентов (по сравнению с 48 процентами заявок USPTO).» См. Patrick Thomas & Dewey Murdick, Patents and Artificial Intelligence: A Primer, Center for Security and Emerging Technology at 10 (Sept. 2020), https://cset.georgetown.edu/wp-content/uploads/CSET-Patents-and-Artificial-Intelligence.pdf. В 2019 году в Китае также было зарегистрировано почти два миллиона заявок на полезную модель. Удостоверение личности № 17.

«Китай выполнил свою стратегическую политическую задачу по увеличению количества своих патентных заявок и выданных патентов, создав представление о том, что он «выиграл» инновационную гонку.»

В-третьих, независимо от проблем с качеством, многочисленные заявки на патенты Китая могут ещё больше навредить американским инноваторам, создав огромный резервуар «предшествующего уровня техники» (термин в патентном праве для обозначения мировых научно-технических знаний, с помощью которых оценивается изобретение, чтобы определить, является ли оно новым). Это резко увеличивает количество предшествующего уровня техники, которое должно быть рассмотрено при рассмотрении патентной заявки. В результате процесс патентной экспертизы в ВПТЗ США будет становиться все более сложным, если не обременительным. В то же время

США изобретателям может быть труднее получить патенты, поскольку они должны показать, что их изобретения не раскрываются в публикациях по предшествующему уровню техники в любой точке мира, в том числе в патентных заявках на китайском языке, поданных в Китае и на международном уровне. По мере того как китайские патенты будут доминировать в поиске предшествующего уровня техники патентными ведомствами по всему миру, нынешнее доминирование американских патентов в мировом поиске предшествующего уровня техники будет разрушаться.

В-четвертых, в соответствии с обширными патентными заявками Китая, китайские компании идентифицируют слишком много патентов как «стандартно необходимые» в организациях по разработке стандартов, утверждая, что эти пациенты должны практиковаться, чтобы соответствовать техническому стандарту. Хотя организации по разработке стандартов требуют от патентообладателей самоидентификации патентов, которые могут быть признаны существенными в будущих стандартах, эти организации оставляют окончательные определения существенности частным компаниям, ведущим переговоры о лицензиях или, в случае возникновения спора,, в суды. Эта практика «сверхдекларирования» стандартных патентов (SEP) способствует глобальному повествованию Китая о том, что он «выиграл» гонку за такими стандартизированными технологиями, как 5G, побуждая другие страны внедрять китайские технологии в свои собственные коммуникационные инфраструктуры. Тревожным результатом может быть то, что американские компании должны выплатить миллиарды роялти китайским компаниям или столкнуться с претензиями и последующими судебными разбирательствами, которые они умышленно нарушили патентные права китайских компаний. В-пятых, отсутствие чёткой правовой защиты данных или чёткой политики в отношении владения данными может препятствовать инновациям и сотрудничеству, особенно по мере развития технологий.

Отсутствие режимов защиты данных может лишить стороны возможности делать необходимые инвестиции в разработку наборов данных,

имеющих решающее значение для систем машинного обучения (ОД) и искусственного интеллекта. Дополнительно, отсутствие политики управления данными (например, передовой практики заключения контрактов) в отношении защиты ИС или правил собственности может подорвать готовность компаний вступать в государственно-частные партнёрства, которые имеют решающее значение для создания передовых технологических инноваций. Это также может создать проблемы для сотрудничества США с союзниками и другими партнёрами в жизненно важных исследованиях и разработках в области ИИ, где права на данные или права собственности ставятся под вопрос.

Наконец, в качестве ещё одного доказательства того, что Китай рассматривает ИС как важнейшую составляющую своего внутреннего экономического развития, Китай продолжает всепроникающе красть американские технологические достижения, защищённые ИС, с помощью различных средств, таких как кибер-взлом предприятий и научно-исследовательских институтов, технологический шпионаж, шантаж и незаконная передача технологий.

«Китай продолжает всепроникающе красть американские технологические достижения, защищённые IP, с помощью различных средств, таких как кибер-взлом предприятий и исследовательских институтов, технологический шпионаж, шантаж и незаконная передача технологий.»

Политика IP Недействительна.

Правительство США должно устранить эти уязвимости, вызванные отсутствием всеобъемлющей политики в области ИС. В настоящее время правительство США недостаточно эффективно использует политику ИС в качестве инструмента поддержки национальных стратегий обеспечения национальной безопасности, экономических интересов и технологической конкурентоспособности в области ИИ и новых технологий. Большинство скоординированных усилий правительства Соединённых Штатов в области политики в области ИС сосредоточены на обеспечении соблюдения прав ИС и предотвращении кражи ИС. Однако в США отсутствует ведомство или

межведомственная структура, наделённая полномочиями как разрабатывать, так и осуществлять национальную политику в области ИС, которая поддерживала бы и интегрировала её с национальными стратегиями.

В результате в Соединённых Штатах отсутствует согласованная, законодательно санкционированная политика в области ИИ и новых технологий в области ИС, которая была бы интегрирована в национальные стратегические рамки для борьбы, например, с глобальной конкуренцией со стороны таких стран, как Китай.

Американские законы и институты в области ИС должны рассматриваться как важнейшие компоненты защиты интересов национальной безопасности США, включая содействие экономическому процветанию и технологической конкурентоспособности. Соединённые Штаты должны, как минимум, сформулировать и разработать национальные реформы и политику в области ИС с целью стимулирования, расширения и защиты ИИ и новых технологий как внутри страны, так и за рубежом. Такая политика должна разрабатываться и предлагаться через Исполнительную власть с помощью процесса, объединяющего разрозненные департаменты и агентства, которые играют важную роль в продвижении инноваций в США. Исполнительная власть должна:

«Американские законы и институты в области ИС должны рассматриваться как важнейшие компоненты защиты интересов национальной безопасности США, включая продвижение экономического процветания и технологической конкурентоспособности.»

Разработка и реализация национальной политики в области ИС для стимулирования, расширения и защиты ИИ и новых технологий. Президент должен издать исполнительный указ о признании ИС национальным приоритетом и потребовать разработки всеобъемлющего плана реформирования и создания политики и режимов в области ИС, способствующих национальной безопасности, экономическим интересам и стратегиям технологической конкурентоспособности. Комиссия рекомендует,

чтобы исполнительный указ поручил вице-президенту в качестве председателя Совета по конкурентоспособности технологий (TCC) или иным образом в качестве председателя межведомственной целевой группы осуществлять надзор за этой работой. Исполнительный указ должен поручить министру торговли в координации с заместителем министра торговли по интеллектуальной собственности и директором USPTO разработать предложения по реформированию и установлению новых политик и режимов ИС, по мере необходимости, для стимулирования, расширения и защиты ИИ и новых технологий. План должен включать предложения по исполнительным и законодательным действиям по изменению политики в области ИС для достижения этих целей и должен сопровождаться оценкой неисчерпывающего перечня «соображений в области ИС».Исполнительный указ должен поручить вице-президенту оценить, какие политики, режимы и предложения по реформированию ИС от Министра торговли должны быть интегрированы в стратегии национальной безопасности, экономической и технологической конкурентоспособности и наделить Министра торговли полномочиями содействовать реализации таких предложений.

Национальные соображения в Области интеллектуальной Собственности.

Защита демократических ценностей: Неприкосновенность частной жизни, гражданские свободы и гражданские права при использовании ИИ в интересах национальной безопасности

План действий

США нужен подход к внедрению ИИ внутри страны для обеспечения национальной безопасности, который поддерживает и укрепляет уважение к демократическим ценностям, включая неприкосновенность частной жизни, гражданские свободы и гражданские права. Такой подход должен укреплять, обеспечивать и демонстрировать лидерство в отношении: 1) прозрачности; 2) подходов к разработке и тестированию систем ИИ; 3) способности оспаривать

решения ИИ; 4) надзора за разработкой и использованием ИИ; 5) законодательного и нормативного контроля за использованием ИИ. Наши рекомендации включают в себя немедленные действия, которые должны предпринять Президент, Конгресс и агентства; всестороннюю оценку Целевой группы, которая приведет к реформам в области управления и надзора за ИИ; области для дальнейшей работы. Рекомендации направлены на обеспечение того, чтобы системы ИИ, используемые органами национальной безопасности, поддерживали демократические ценности. Во-вторых, принятие этих рекомендаций может завоевать и внушить доверие общественности, как внутри страны, так и за рубежом, к использованию ИИ органами национальной безопасности.

Набор рекомендаций 1: Повышение общественной прозрачности использования ИИ за счет улучшения отчётности

Действия для Конгресса:

• Для систем ИИ, в которых участвуют лица из США, требуются Отчеты об оценке рисков ИИ и Оценки воздействия ИИ для оценки последствий конфиденциальности, гражданских свобод и гражданских прав для каждой новой квалифицирующей системы ИИ или значительного обновления системы.

Комиссия предлагает Конгрессу потребовать от Разведывательного сообщества (координируемого Канцелярией директора национальной разведки (ODNI)), а также Министерства внутренней безопасности (DHS) и Федерального бюро расследований (ФБР) подготовить и опубликовать Отчет об оценке рисков ИИ и провести оценку воздействия ИИ для оценки последствий конфиденциальности, гражданских свобод и гражданских прав каждой новой квалифицирующей системы ИИ или значительного обновления системы. Комиссия признает текущие требования к оценке воздействия на частную жизнь и оценке воздействия на гражданские свободы, проводимые в агентствах в соответствии с требованиями действующего устава. Технологии, связанные с ИИ, могут быть пересмотрены ими, но не полностью (адекватно)

охвачены текущими оценками. Рекомендация Комиссии направлена на расширение этих требований.

Отчет об оценке рисков ИИ и Оценка воздействия ИИ потребуются для «новых квалификационных систем ИИ» и для «значительного обновления системы.» Комиссия предлагает поручить Целевой группе, описанной далее в этом Плане, определить процедуры принятия решений для определения того, какие системы ИИ и значительные обновления систем потребуют отчетов об оценке рисков и последствий ИИ.

Цель Отчета об оценке рисков ИИ и Оценки воздействия ИИ состоит в том, чтобы обеспечить учет и смягчение потенциальных воздействий, избегая при этом ненужного увеличения бремени соблюдения требований.

Законодательно закреплённые рамки обеспечения эффективного и прагматичного снижения рисков (с возможностью категоризации систем по рискам и определения соответствующих мер по снижению рисков, если таковые имеются) существуют и в других моделях, которые могут быть использованы в качестве шаблона (например, FISMA).

Отчет об оценке рисков ИИ должен включать подробный анализ системных последствий и шагов по снижению и отслеживанию рисков (например, с помощью метрик):

Свобода выражения мнений (например, является ли слежка с поддержкой ИИ нацеленной на людей из-за их деятельности, защищенной Первой поправкой, или правительственная слежка с поддержкой ИИ вызывает или потенциально может вызвать пугающий эффект?);

Равная защита (например, является ли наблюдение с поддержкой ИИ предвзятым по отношению к защищенному классу? Каковы вероятные последствия новой технологии или программы для ключевых демографических показателей, таких как раса, пол или инвалидность?);

Конфиденциальность (например, требуется ли ордер на действия правительства? Являются ли процессы минимизации и запроса достаточными/удовлетворительными?);

Возмещение ущерба и надлежащая правовая процедура (например, какие существуют механизмы или были приняты ограничения для предоставления возмещения за неблагоприятные действия правительства, предпринятые на основе информации, генерируемой системой искусственного интеллекта?);

Оценка должна учитывать среду, в которой будет развернута система ИИ, включая ее взаимодействие с другими инструментами и программами ИИ, которые собирают личную идентифицируемую информацию (PII).

Оценка воздействия ИИ должна периодически, но не реже одного раза в год, предоставляться Управлению агентства по вопросам конфиденциальности и гражданских свобод (PCL) для определения степени соответствия квалификационной системы ИИ ограничениям и показателям, установленным в Оценке рисков. Оценки воздействия ИИ должны основываться на результатах, воздействиях и метриках, собранных в ходе использования системы, и определять, следует ли совершенствовать существующие процессы валидации.

Ресурсы и персонал. Отделениям ПКЛ следует оценить ресурсы, включая персонал, необходимые для адекватного выполнения вышеуказанных задач. Руководители учреждений должны поддерживать дополнительные ресурсы для отделений PCL в рамках годового бюджетного процесса.

Уведомления о раскрытии информации. Конгресс должен потребовать от ODNI, DHS и ФБР пересмотреть непубличные и/или секретные программы ИИ, как только программа будет закрыта для рассекречивания и/или раскрытия.

Действия для президента:

• Если Конгресс не потребует новых отчетов о конфиденциальности, гражданских свободах и гражданских правах (как указано выше), проведите Оценку рисков ИИ и Отчеты об оценке воздействия ИИ, как описано выше.

Действия для DHS и ФБР:

• DHS и ФБР должны ввести новые обязательства в отношении Системы уведомлений о регистрации (SORN) и Оценки воздействия на конфиденциальность (PIA), специфичных для систем ИИ, чтобы гарантировать, что они предоставляют более богатую информацию.

SORNs и PIA должны предоставлять целостную картину о сборе, использовании и хранении личной информации любой системой ИИ, включая ее связи с существующими системами и учет наслоения различных технологий наблюдения, где это применимо. Агентская практика не в достаточной степени поддерживает производство SORN и PIA, которые адекватно описывают, как системы ИИ собирают, используют и хранят личную информацию.

DHS и ФБР должны требовать, чтобы все PIA включали описание используемого алгоритма(ов) и цели алгоритма(ов); потенциал для вывода дополнительной информации о лицах из агрегирования нескольких источников данных; и, что важно, меры, которые будут использоваться для устранения этих рисков.

DHS и ФБР должны требовать от SORNS большей конкретности в описании типов собираемых данных, источников данных и связей между источниками данных, а также того, кто будет использовать такие данные и почему.

• DHS и ФБР должны предпринять шаги для повышения прозрачности общественности в отношении систем искусственного интеллекта, которые они используют.

DHS недавно приступила к работе по повышению прозрачности, и эти усилия должны быть приоритетными и оцениваться по мере их реализации.

ФБР должно провести аналогичные реформы для повышения прозрачности.

• DHS и ФБР должны сделать свои веб-сайты более удобными для общественности и обеспечить регулярное обновление веб-сайтов. Отчеты об оценке рисков и последствий для частной жизни, гражданских свобод и гражданских прав, связанные с ними полугодовые отчеты, PIA и SORN должны располагаться в центральном месте, иметь четко обозначенные даты рядом с названием, а также быть хронологически упорядочены и своевременно публиковаться. DHS и ФБР должны ежегодно запрашивать публичные комментарии о навигации своих веб-сайтов и потенциальных улучшениях.

Набор рекомендаций 2: Разработка и тестирование систем в соответствии с Целями сохранения конфиденциальности и справедливости

Действия для Президента:

• Президент своим Указом должен потребовать от директора национальной разведки, министра внутренней безопасности и директора ФБР принять следующие меры:

• Осуществлять шаги по снижению рисков конфиденциальности, гражданских свобод и гражданских прав, связанных с любой системой искусственного интеллекта, на итеративной основе и требовать документирования всех принятых рисков.

При осуществлении шагов по достижению этой цели Комиссия рекомендует ODNI, DHS и ФБР применять практику, основанную на Ключевых соображениях. В частности:

Используйте средства защиты конфиденциальности, такие как надежная анонимизация, способная противостоять сложным атакам повторной идентификации, и, когда это возможно, технологии сохранения конфиденциальности, такие как дифференциальная конфиденциальность, федеративное обучение и машинное обучение (мл) с шифрованием данных и моделей.

Смягчайте предвзятость при разработке и тестировании. Что касается развития, то проведите взаимодействие с заинтересованными сторонами, чтобы установить консенсус по определению показателей справедливости, которые будут использоваться для конкретного развития и определить необходимые ограничения на поведение системы для защиты гражданских прав и предотвращения несправедливых результатов. При тестировании убедитесь, что определенные ограничения выполняются. Тестирование для выявления непреднамеренной предвзятости должно включать в себя тестирование и документирование различных типов ошибок (например, различий в ложноположительных или ложноотрицательных показателях) или несопоставимых результатов в разных демографических группах.

Используйте ИИ-инструменты для поддержки оценки справедливости (например, отраслевые инструменты, упомянутые в Ключевых соображениях).

Убедитесь, что цепочки инструментов Mips включают рутинную калибровку согласованных показателей справедливости на протяжении всей непрерывной разработки и интеграции.

Оценивайте эффективность модели и влияния системы во время полевых работ на постоянной основе, включая эмерджентное поведение, для обеспечения соответствия целям конфиденциальности, гражданских прав и гражданских свобод.

• Назначьте офис, комитет или группу в каждом агентстве для проведения предварительного обзора технологий ИИ, которые повлияют на конфиденциальность, гражданские свободы и гражданские права, включая соответствующую документацию.

Это должно включать проверку перед их развертыванием, в том числе на соответствие требованиям в течение всего срока службы системы. В каждом агентстве разведывательного сообщества, DHS и ФБР должен быть оборудован офис для оценки данных, моделей и системной документации, а также результатов тестирования технологий в соответствии с их предполагаемым использованием.

При проведении этого обзора Комиссия рекомендует назначенному ведомству использовать Ключевые соображения.

Действия для Конгресса:

• Создать сторонний центр (центры) тестирования, чтобы позволить независимому стороннему тестированию систем ИИ, связанных с национальной безопасностью, и которые могут повлиять на американских граждан.

Конгресс должен финансировать NIST для создания Сторонней программы Лаборатории тестирования ИИ в рамках Национальной программы добровольной аккредитации лабораторий NIST.

Мандат механизма тестирования третьей стороны должен заключаться в следующем:

Индивидуальная метрическая оценка в зависимости от миссии и полномочий агентства;

Разработать подход к тестированию как программных продуктов, которые могут быть установлены в тестовом центре, так и облачных сервисов;

Установить обязательные соглашения о распространении данных с заинтересованными сторонами тестируемой системы (например, агентством, запрашивающим тестирование, и соответствующими поставщиками и владельцами данных);

Сотрудничайте с агентством, занимающимся тестированием, чтобы достичь консенсуса относительно того, как обращаться с предоставленными тестовыми данными, а также с результатами испытаний и отчётами.

Сторонние тестовые центры должны позволять государственным поставщикам обмениваться собственными данными, не опасаясь, что они будут раскрыты конкурентам, и предлагать преимущества агрегированного представления результатов деятельности по всему сектору или совокупности корпораций и агрегированного передового опыта.

Сторонние испытательные центры должны использоваться агентствами до приобретения или внедрения систем с высокими последствиями, влияющих на американских граждан, и их использование должно рассматриваться как преодоление внутренних ограничений тестирования.

• Потребовать от Министерства юстиции (DOJ) в консультации с Советом по надзору за неприкосновенностью частной жизни и гражданскими свободами (PCLOB) разработать обязательное руководство по использованию сторонних тестов (например, пороговые значения для систем с высокими последствиями или беспрецедентные факторы) систем ИИ.

Это должно включать критерии того, когда система ИИ может представлять достаточно высокий риск для частной жизни, гражданских свобод и гражданских прав, чтобы она вызвала требование тестирования третьей стороной. При формировании такого руководства PCLOB и Министерство

юстиции должны консультироваться с сотрудниками PCL в федеральных агентствах.

Признание продолжающейся работы технического сообщества и экспертов по правовым вопросам.

Существуют значительные нерешенные противоречия между различными техническими подходами к сохранению гражданских прав и гражданских свобод и существующими и ожидаемыми правовыми рамками. Например, ученые выразили обеспокоенность тем, «что технические и правовые подходы к смягчению предвзятости будут настолько расходиться, что законы, запрещающие алгоритмическую предвзятость, не смогут на практике отсеять предвзятые алгоритмы, а технические методы, предназначенные для устранения алгоритмической предвзятости, будут считаться незаконно дискриминационными.» Необходимо продолжать работу в технической, правовой и политической областях, чтобы найти согласованный баланс, который касается технических подходов к сохранению частной жизни, гражданских свобод и гражданских прав и эволюционирующей политики.

Рекомендация 3: Закрепить возможность лиц, пострадавших от ИИ, добиваться возмещения ущерба и соблюдения надлежащей правовой процедуры.

Действия для ФБР и DHS:

• ФБР и DHS должны провести обзор своей соответствующей политики и практики, связанной с технологией ИИ, чтобы гарантировать, что стороны, пострадавшие от действий правительства, связанных с использованием ИИ, в том числе в результате системных действий или неправильного использования, могут добиваться возмещения ущерба и четко знать, как это сделать. По крайней мере, ежегодно ФБР и DHS должны оценивать, требуются ли обновления или изменения в их соответствующих обзорах.

Этот обзор должен определить, адекватно ли предоставляется уведомление об использовании ИИ в процессе принятия решений потерпевшим

сторонам для обеспечения возмещения ущерба, а также степень проверяемости и интерпретируемости, необходимых для оспаривания.

Группа проверки ФБР и/или DHS, в состав которой должно входить Управление по вопросам конфиденциальности и гражданских свобод, должна представить рекомендации руководителям соответствующих ведомств относительно любых нормативных и/или политических изменений, необходимых для внесения поправок в существующие механизмы возмещения ущерба с учетом проблем, возникающих в связи с использованием системы с поддержкой искусственного интеллекта.

Генеральный прокурор, работая с директором ФБР и министром внутренней безопасности, соответственно, должен направлять соответствующие указания в целях обеспечения каждым ведомством:

адекватного возмещения ущерба на основе рекомендаций обзора;

предоставления общественности четких, обновлённых рекомендаций о том, как добиваться возмещения ущерба в ситуациях, охватываемых обзором, в том числе путем размещения соответствующей информации на своих веб-сайтах.

Действия для Генерального прокурора:

• Издать федеральное руководство по ИИ и надлежащей правовой процедуре. В этом руководстве должно быть описано, как соответствующие ведомства должны защищать процессуальные права граждан США, когда использование ИИ может привести к лишению жизни или свободы. Это должно включать в себя обязательства агентств своевременно раскрывать информацию об использовании ИИ обвиняемому по уголовному делу до судебного разбирательства или слушания (т.е. обязательства по уведомлению), включая роль, которую ИИ сыграл, приведя к аресту, обвинению или уголовному преследованию. Такие руководящие указания должны быть включены в оперативные руководящие принципы агентства.

Признание продолжающейся работы судебной и/или законодательной ветвей власти:

Вышеупомянутые действия должны обеспечить получение агентствами чётких указаний по возмещению ущерба, связанного с ИИ, и надлежащему процессуальному процессу в промежуточный период, когда Конгресс и/или суды взвешивают федеральные требования. Необходимо будет продолжить работу по обеспечению базового руководства эволюцией возможностей ИИ и их применением, а также в рамках решения открытых вопросов о федеральных правилах доказывания и уголовного судопроизводства, касающихся ИИ.

Группа рекомендаций 4: Укрепление механизмов надзора и управления для решения текущих и меняющихся проблем

Действия для Конгресса:

• Закрепить возможность Совета по надзору за неприкосновенностью частной жизни и гражданскими свободами (PCLOB) в части обеспечения значимого надзора и консультирования федерального правительства по использованию технологий с поддержкой ИИ в контртеррористических целях. Для достижения этой цели Конгресс должен предусмотреть целенаправленное расширение полномочий и ассигнований PCLOB следующим образом:

Осведомленность о программах ИИ. В рамках полномочий PCLOB, обеспечивающих доступ ко всем соответствующим материалам от агентств, агентства должны быть обязаны предоставлять PCLOB уведомление до внедрения или перепрофилирования системы искусственного интеллекта, а также любые связанные с этим оценки воздействия на частную жизнь, гражданские свободы и гражданские права.

Видимость в технологии. Агентства должны быть обязаны предоставлять PCLOB по запросу PCLOB конкретную информацию о технологиях, используемых в любой системе ИИ, включая: данные, используемые для систем ИИ (например, документацию, касающуюся процессов сбора данных для инструментов и программ с поддержкой ИИ, включая процессы раскрытия и согласия); используемые модели (и вспомогательную модельную документацию, касающуюся обучения и тестирования); перепрофилирование

моделей (за пределами того контекста, для которого они были подготовлены/одобрены).

Ресурсы и другие организационные потребности. PCLOB требует увеличения своих ресурсов, как с точки зрения талантов, так и финансирования, чтобы достичь своей миссии и управлять своим портфелем по мере роста внедрения ИИ. PCLOB должен предоставить Конгрессу самооценку своих ресурсов и организационной структуры с учётом ожидаемого увеличения числа программ, связанных с ИИ, которые подпадают под его нынешний мандат и обязанности.

• Расширение прав и возможностей отделов DHS по вопросам неприкосновенности частной жизни, гражданских прав и гражданских свобод. Конгресс должен усилить роль Управления по вопросам конфиденциальности DHS и Управления по гражданским правам и гражданским свободам, обязав Главного сотрудника по гражданским правам и гражданским свободам, в координации с Сотрудником по вопросам конфиденциальности, играть неотъемлемую роль в юридических процессах и процессах утверждения закупок и использования систем с поддержкой искусственного интеллекта, включая связанные с ними данные систем машинного обучения в DHS. В рамках этого законодательства бюро по вопросам неприкосновенности частной жизни, гражданских прав и гражданских свобод должны отчитываться перед Конгрессом о дополнительных кадровых или финансовых ресурсах, необходимых для выполнения этого мандата.

Меры в интересах министра внутренней безопасности

• Обеспечить получение Сотрудником по вопросам конфиденциальности и кругу сотрудников постоянных мест в новом общеорганизационном координационно-консультативном совете по ИИ DHS. Такие назначения необходимы для того, чтобы осмысленно удовлетворить цель Стратегии DHS AI под названием «Формализация процессов управления ИИ в DHS.»

Действия для Президента:

• Посредством Исполнительного указа потребовать более тесной координации и согласования действий надзорных и аудиторских организаций путем создания межведомственной рабочей группы, занимающейся вопросами надзора и аудита. Добровольное соблюдение учреждениями требований к документации и тестированию ИИ должно подкрепляться строгим, технически обоснованным надзором. Для достижения этой цели и преодоления существующих препятствий в области аудита постоянный орган (например, межведомственная рабочая группа) должен согласовывать и координировать усилия по усилению надзора и аудита ИИ в отношении конфиденциальности, гражданских свобод и гражданских прав. Это включает в себя проверку системы таким образом, чтобы правительство могло контролировать и отслеживать шаги, которые привели к выходу системы, и проводить аудит, чтобы системы не использовались неправильно.

Состав: Организации должны включать Секцию по надзору за разведывательной деятельностью Министерства юстиции; Управление генерального инспектора разведывательного сообщества; Управление по подотчетности правительства; Совет по надзору за частной жизнью и гражданскими свободами; Управление по гражданским свободам и частной жизни органов национальной безопасности; Совет национальной безопасности и Управление научно-технической политики.

Функция: Межведомственная рабочая группа должна служить форумом для того, чтобы ее члены могли предметно и регулярно обсуждать и обмениваться информацией. Рабочая группа должна:

Разработать перечень видов надзора и аудита, связанных с ИИ, которые в настоящее время осуществляются организациями-участниками и ожидаются ими.

Разработать перечень конкретных возможностей, разработанных в каждой организации для решения вопросов надзора и аудита ИИ.

Оценка имеющихся инструментов с поддержкой искусственного интеллекта, которые могут быть адаптированы для поддержки более эффективного и действенного надзора и аудита.

• Инструменты, поддерживающие финансовый аудит и модельное управление рисками, являются примерами достижений применения ИИ для повышения эффективности и масштабируемости аудитов, которые должны быть пересмотрены для принятия.

Определить приоритетные инвестиционные потребности для каждой организации для удовлетворения текущих потребностей.

Определить приоритетные темы исследований для открытых научно-технических пробелов в поддержке надзора и аудита ИИ, включая пробелы в исследованиях применения ИИ в поддержку конфиденциальности и гражданских свобод (например, методы ОД для классификации, рекомендации, обнаружения аномалий и другие приложения) и расширить инструменты, которые поддерживают финансовый аудит и модельное управление рисками;

Рекомендовать политические или законодательные изменения для конкретных полномочий, предоставленных отдельным организациям.

Устраните дублирование задач и фокусов между репрезентативными организациями.

Выпускать отчеты, как минимум ежегодно, о ключевых надзорных и аудиторских мероприятиях, а также о научно-технических пробелах.

Действия для Президента или Конгресса:

• Создать целевую группу для оценки последствий ИИ и новых технологий для частной жизни, гражданских прав и гражданских свобод.

Цель целевой группы состояла бы в выявлении пробелов и выработке рекомендаций по обеспечению использования ИИ и связанных с ним данных в соответствии с американскими законами и ценностями в операциях правительства США, а также в изучении организационных реформ, которые способствовали бы достижению этой цели. В частности, она должна оценить

существующие политические и правовые пробелы в отношении существующих приложений ИИ и новых технологий и вынести рекомендации по:

• законодательным и нормативным реформам в области разработки и внедрения ИИ и новых технологий;

• институциональным изменениям для обеспечения постоянной оценки и постоянного руководства по вопросам конфиденциальности и гражданских свобод, связанных с применением ИИ и новыми технологиями.

Как упоминалось в главе 8 настоящего доклада, развитие ИИ требует перспективного подхода к надзору, который предвосхищает дальнейшую эволюцию и внедрение новых технологий, а также позволяет правительству более ответственно управлять их занятостью в будущем. Комиссия считает, что для достижения этой цели необходима новая целевая группа.

Комиссия рекомендует Президенту или Конгрессу создать целевую группу с предлагаемым членским составом, структурой, функциями и приоритетами, указанными ниже.

Для целесообразности Президент должен:

• Издать Исполнительный указ о создании целевой группы, которой будет поручено рекомендовать реформы в области управления и надзора за ИИ.

Членство и структура. Президент должен создать целевую группу в Исполнительном аппарате Президента для разработки рекомендаций по обеспечению надлежащего управления и надзора за ИИ. Председатель должен назначить старшего должностного лица для руководства целевой группой. В ее состав должны входить руководители OMB, NIST, PCLOB и GAO, а также главные сотрудники по гражданским свободам и неприкосновенности частной жизни и генеральные инспекторы всех агентств национальной безопасности. Кроме того, в состав целевой группы должны входить представители гражданского общества (включая руководителей организаций, обладающих опытом в области частной жизни, гражданских свобод и гражданских прав), промышленности и научных кругов. Следует также представить Подкомитет

Национального консультативного комитета по ИИ и правоохранительным органам.

Функция. На целевую группу должны быть возложены следующие обязанности:

Проведение макрооценки влияния возможностей ИИ и новых технологий на частную жизнь и гражданские права и гражданские свободы;

Выработка рекомендаций по законодательным и нормативным реформам в области разработки и внедрения ИИ и новых технологий, включая связанные с ними данные, в следующих ключевых областях:

• Отчетность о конфиденциальности, гражданских свободах и гражданских правах (P/CLCR). Обязательное руководство о том, когда IC, DHS и ФБР должны подготовить и опубликовать Отчет об оценке риска ИИ и Оценки воздействия ИИ, в частности, что представляет собой квалифицирующую систему ИИ или значительное обновление системы (как обсуждается в первой рекомендации главы 8 настоящего отчета).

• Биометрические технологии. Это должно включать базовые стандарты для использования федеральным правительством технологий биометрической идентификации, включая, но не ограничиваясь этим, распознавание лиц.

Для решения насущной потребности в базовых стандартах и гарантиях в отношении распознавания лиц это должно включать оценку пробелов в федеральном законодательстве, сбор информации от заинтересованных сторон агентства (и их юридических консультантов), использующих в настоящее время распознавание лиц для миссий национальной безопасности; экспертов по вопросам конфиденциальности, гражданских свобод и гражданских прав внутри и за пределами правительства, включая PCLOB; а также от общественности в целом для выработки рекомендаций по законодательству о распознавании лиц.

Помимо распознавания лиц, потребуется руководство в отношении других инструментов биометрической идентификации, включая голосовые отпечатки.

• Государственные закупки коммерческой продукции. Это должно включать в себя контрактную передовую практику обеспечения того, чтобы отраслевые продукты ИИ (включая связанные с ними данные), закупаемые правительством, поддерживали конфиденциальность, гражданские свободы и ожидания гражданских прав (включая конфиденциальность, информационную безопасность, справедливость/недискриминацию, проверяемость и подотчетность). Это должно включать требования третьих сторон, которые должны быть включены в условия закупок, касающиеся ответственных целей ИИ, в том числе для проверки валидации тестирования.26 Следует рассмотреть вопрос как о государственных закупках, так и о коммерческих закупках (COTS).

• Конфиденциальность и хранение данных. Обновление и реформирование требований к конфиденциальности и хранению государственных данных для решения проблем, связанных с ИИ.

Выработка рекомендаций по институциональным изменениям для обеспечения устойчивой оценки и постоянного руководства по последствиям применения ИИ и новых технологий для конфиденциальности и гражданских свобод.

• Развивающиеся возможности ИИ готовы бросить вызов существующим ожиданиям в отношении конфиденциальности, гражданских свобод и гражданских прав. В свете этого целевая группа должна оценить полезность нового органа в рамках федерального правительства для регулирования и обеспечения общегосударственного надзора за использованием ИИ федеральным правительством.

• При оценке вариантов создания нового подразделения целевой группе следует учитывать следующее:

Полномочия и ресурсы, необходимые новому органу для обеспечения постоянного руководства и базовых стандартов для:

Разработку, приобретение и внедрение технологий искусственного интеллекта федеральным правительством для обеспечения их соответствия

законодательству и ценностям в области конфиденциальности, гражданских свобод и гражданских прав, а также для включения барьеров по использованию запрещённых результатов, которые должны быть включены в политику и встроены в разработку систем;

Прозрачность для надзорных органов и общественности в отношении использования федеральным правительством систем искусственного интеллекта и эффективности этих систем;

Существующие межведомственные и внутриведомственные усилия по решению проблемы надзора за ИИ;

Уникальные потребности национальной безопасности, правоохранительных органов и других правительственных миссий в отношении систем искусственного интеллекта и потенциальные последствия для частной жизни, гражданских свобод, гражданских прав и гражданских свобод;

• Формулировку рекомендаций по организационному размещению и структуре, составу, полномочиям и необходимым ресурсам после рассмотрения потенциальной полезности новой организации;

Оценку текущих усилий по адаптации регулирования внедрения ИИ в частном секторе и, при необходимости, рассмотрение и рекомендация институциональных или организационных изменений для содействия адекватному регулированию коммерческой разработки и внедрения ИИ и связанных с ним данных.

Отчет. Целевая группа должна представлять Президенту доклад со своими законодательными и нормативными рекомендациями на скользящей основе, но не позднее чем в течение 180 дней с момента ее создания. Она должна в течение одного года после своего создания представить Президенту доклад с рекомендациями по организационным изменениям. Комиссия рекомендует представить этот доклад Конгрессу для обеспечения транспарентности и оказания Конгрессу помощи в рассмотрении этих важнейших вопросов.

• В качестве альтернативы Конгресс должен санкционировать существование этой целевой группы, как указано выше.

Признание продолжающейся работы по обновлению и уточнению правовой базы по ключевым вопросам защиты данных и конфиденциальности данных:

Комплексный подход к защите частной жизни и гражданских свобод в эпоху искусственного интеллекта требует решения нескольких крупных нерешенных политических и юридических вопросов, касающихся защиты данных и конфиденциальности данных. Подробные рекомендации по этим вопросам выходили бы за рамки мандата этой Комиссии, но мы выделяем их здесь для того, чтобы призвать к дальнейшему изучению и принятию мер Конгрессом.

• Юридические проблемы, связанные с федеральным использованием данных третьих лиц. Конгресс и/или судебные органы должны оценить адекватность существующих правовых ограничений в отношении получения и использования федеральным правительством данных третьих сторон, включая данные, полученные от брокеров данных. Либо благодаря развитию прецедентного права, либо законодательства агентства выиграют от ясности, связанной с применением Четвертой поправки к данным третьих сторон. Тем временем учреждения должны обеспечить прозрачность своей соответствующей политики и правовой базы для доступа к коммерческим данным и их использования.

• Национальные стандарты защиты данных. Политика конфиденциальности данных и стандарты, применимые только к государственным учреждениям, будут неадекватны, а в некоторых случаях могут нанести ущерб интересам национальной безопасности. Это особенно важно с учётом того, как противники (как государственные, так и негосударственные субъекты) могут получить доступ и использовать данные, собранные о лицах США. Поскольку Конгресс рассматривает предложения по национальной безопасности данных и защите частной жизни, он должен

обеспечить рассмотрение любым будущим законодательством проблему микротаргетинга. Как отмечалось, системы искусственного интеллекта создадут новые возможности для государственных субъектов в точном нацеливании людей и в таких многочисленных аспектах нашего общества, как города, цепочки поставок, университеты, корпорации, инфраструктура и финансовые транзакции. Сильная защита конфиденциальности данных будет необходима по множеству причин, в том числе для защиты Соединенных Штатов от этого нового явления.

• Национальные рамки использования биометрических технологий. В отсутствие федерального законодательства, регулирующего использование распознавания лиц, существующее лоскутное одеяло государственных и местных законов и нормативных актов создает ряд трудностей для государственных чиновников, промышленности и общественности. Это привело к таким действиям: компании, запрещающие продажу распознавания лиц правоохранительным органам и запреты местных органов власти на использование распознавания лиц появились от побережья до побережья. За отсутствие последовательного федерального подхода ответственны органы национальной безопасности, когда лучшие практики не используются на местном уровне. При разработке правил крайне важно, чтобы политика и законодательство учитывали не только распознавание лиц, но и другие виды биометрической идентификации, которые в сочетании с другими технологиями искусственного интеллекта могут вызвать дополнительные проблемы.

Нерегулируемый и легальный Сбор данных и посредничество в прогнозировании и идентификации с использованием искусственного интеллекта

Основываясь на основных рекомендациях, содержащихся в Заключительном докладе Комиссии, Планы действий содержат более подробные дорожные карты для действий исполнительной и законодательной ветвей власти по сохранению лидерских позиций Америки в области

искусственного интеллекта. План действий определяет, кто должен предпринять то или иное действие – Конгресс, Белый дом или департамент исполнительной власти или агентство. В рамках своих рекомендаций Комиссия представляет смету увеличения объема финансирования или ассигнований. Все рекомендации, включающие цифры финансирования, должны рассматриваться как смета для рассмотрения Конгрессом и/или Исполнительной властью.

Стратегия конкуренции и сотрудничества

Соединенные Штаты должны продвигать в отношении Китая всеобъемлющую политику, которая поощряет и защищает основанный на правилах международный порядок. Инвестируя в конкурентоспособность и устойчивость США внутри страны, защищая критические технологии и углубляя координацию с союзниками и партнерами, Соединенные Штаты могут продолжать сотрудничество с Китаем – там, где это отвечает национальным интересам и с позиции силы. Должным образом упорядоченная и обеспеченная ресурсами, такая стратегия позволила бы найти решения глобальных проблем и использовать формальный дипломатический диалог для решения важнейших проблем, связанных с новыми технологиями.

Рекомендация: Установить Всеобъемлющий научно-технический диалог между США и Китаем на высоком уровне

Соединенные Штаты должны наладить регулярный технологический диалог на высоком уровне с Китаем, который принесет пользу американскому народу, сохранит верность нашим союзникам и заставит Китай соблюдать международные правила и нормы. Диалог должен быть сосредоточен на проблемах, связанных с новыми технологиями, включая ИИ, биотехнологии и другие технологии, согласованные обеими сторонами. КНТР должна иметь две всеобъемлющие цели:

• Определить целевые области сотрудничества в области новых технологий для решения глобальных проблем, таких как изменение климата, здравоохранение и стихийные бедствия; и

• Обеспечить форум для обсуждения дискретного набора проблем или точек трения вокруг конкретного использования новых технологий при построении отношений и установлении процесса между двумя странами.

Соединенные Штаты должны четко понимать, что диалог не решит всех наших разногласий с Китаем. КНТР должен быть ориентирован на конкретные результаты и должен добиваться конкретных результатов для американского народа.

Действия для Белого дома и Государственного департамента:

• Создание КНТР.

Новые технологии играют важную роль в динамике экономических, социальных отношений и безопасности между Соединенными Штатами и Китаем. Поэтому КНТР следует создать как часть всеобъемлющей стратегии в отношении Китая, которая мобилизует демократических союзников и партнеров в поддержку основанного на правилах международного порядка.

Государственный департамент – в тесной координации с Управлением научно-технической политики должен возглавить КНТР.

Государственный департамент должен выстроить процесс, ориентированный на результат и направленный на решение возможных проблем в нынешних отношениях между Соединенными Штатами и Китаем, связанных с новыми технологиями. Например:

КНТР следует изучить совместные технологические решения глобальных проблем (например, изменение климата, здравоохранение и биологические данные, безопасность пищевых продуктов и стихийные бедствия).

КНТР следует определить области текущих проблем, связанные с новыми технологиями (например, обмен данными и конфиденциальность, управление рисками цепочки поставок, международные стандарты и нормы, а также

интеллектуальная собственность), и разработать четкую дорожную карту с основными этапами решения этих проблем.

КНТР следует инициировать обмен кадрами и механизмы обмена данными для поддержки и содействия выявленным исследовательским проектам с взаимным доступом к информации, которая может привести к конкретным результатам.

Соединенные Штаты должны определить лидирующие позиции по каждой из этих тем (например, Министерство энергетики, Специальный посланник Президента США по климату и Национальное управление океанических и атмосферных исследований по изменению климата; Национальные институты здравоохранения по здравоохранению; Управление по продовольствию и лекарствам США по безопасности пищевых продуктов; Министерство обороны и Агентство США по международному развитию по стихийным бедствиям).

• Отношение к стратегическому диалогу. Отдельно от этого КНТР рекомендовала правительствам Соединенных Штатов и Китая созвать Стратегический диалог по вопросам безопасности (ССБ), направленный на устранение недоразумений и неправильных представлений по ключевым стратегическим вопросам и угрозам и снижение вероятности непреднамеренной эскалации. Китай сопротивлялся попыткам США создать такой диалог в течение почти десяти лет, но его создание никогда не было более критичным. Видение Комиссии в отношении роли ССД более подробно рассматривается в главе 4 настоящего доклада.

Этот диалог должен стать основным форумом для обсуждения практики, связанной с использованием ИИ и автономных систем вооружения, и должен включать обсуждение испытаний, доктрины и применения, а также, возможно, изучение практических конкретных мер укрепления доверия для снижения рисков.

Важно отделить ССД от КНТР, чтобы обеспечить изоляцию дискуссий, связанных с эскалацией конфликтов и кризисной стабильностью, от

политических сил, влияющих на более широкие двусторонние отношения между США и Китаем.

Проект Указа о создании Совета по технологической конкурентоспособности

В соответствии с полномочиями, предоставленными мне как Президенту Конституцией и законами Соединенных Штатов Америки, и в целях обеспечения скоординированного процесса разработки технологической политики и национальной технологической стратегии и контроля за ее осуществлением, настоящим учреждается:

Раздел 1. Политика. Национальная безопасность, экономическая конкурентоспособность и внутреннее процветание Соединенных Штатов требуют комплексного и скоординированного подхода федерального правительства к обеспечению долгосрочного лидерства США во всём комплексе критических и новых технологий. Для достижения этой цели настоящим Указом учреждается Совет по конкурентоспособности технологий для разработки Национальной технологической стратегии и координации политики в отношении критических и новых технологий в рамках Федерального правительства.

Раздел. 2. Совет по конкурентоспособности технологий.

(a) Учреждение. Создание Совета по технологической конкурентоспособности (Council).

(b) Членство. Совет состоит из следующих членов:

(i) вице-президент, который является Председателем Совета;

(ii) Государственный секретарь;

(iii) Секретарь казначейства;

(iv) Министр обороны;

(v) Генеральный прокурор;

(vi) Министр торговли;

(vii) Министр энергетики;

(viii) Министр внутренней безопасности;

(ix) директор Управления по вопросам управления и бюджета;

(x) помощник Президента по вопросам технологической конкурентоспособности;

(xi) помощник Президента по вопросам национальной безопасности;

(xii) помощник Президента по науке и технике;

(xiii) помощник Президента по экономической политике;

(xiv) помощник Президента по внутренней политике;

(xv) торговый представитель Соединенных Штатов;

(xvi) председатель Объединенного комитета начальников штабов;

(xvii) руководители других исполнительных департаментов и учреждений и другие старшие должностные лица в составе канцелярии Президента, определяемые Председателем.

Член Совета может назначить для выполнения функций члена Совета должностное лицо высшего уровня, входящее в состав департамента, агентства или члена канцелярии и являющееся штатным должностным лицом или служащим Федерального правительства.

(c) обязанности Председателя.

(i) Председатель или, по его или ее указанию, помощник Председателя по вопросам технологической конкурентоспособности созывает заседания Совета и председательствует на них, а также определяет повестку дня Совета.

(ii) Председатель санкционирует создание таких комитетов Совета, как исполнительный комитет, и таких рабочих групп, состоящих из назначенных старших членов Совета и других должностных лиц, приглашенных для участия в заседаниях Совета, которые он или она сочтет необходимыми или целесообразными для эффективного выполнения функций Совета.

(iii) Председатель докладывает о деятельности и рекомендациях Совета. Председатель консультирует Совет по мере необходимости относительно указаний Президента в отношении деятельности Совета и технологии национальной политики в целом.

(d) Административное управление.

(i) Совет имеет штат, возглавляемый помощником Президента по вопросам технологической конкурентоспособности.

(ii) Административное управление в Административной канцелярии Президента предоставляет Совету этот персонал, финансирование и административную поддержку в пределах, разрешённых законом, и при условии наличия ассигнований, по указанию Председателя или помощника Президента, по вопросам технологической конкурентоспособности для выполнения положений настоящего приказа.

(iii) В той мере, в какой это практически осуществимо и разрешено законом, включая Закон об экономике, и в рамках существующих ассигнований учреждения, работающим в Совете предоставляются ресурсы, включающие кадровую и служебную поддержку, но не ограничивающиеся этим по обоснованной просьбе Председателя или, по указанию помощника Президента по вопросам технологической конкурентоспособности.

(iv) Руководители учреждений предоставляют, в соответствующих случаях и в пределах, разрешенных законом, такую помощь и информацию Совету, какую Председатель может запросить для выполнения настоящего распоряжения.

(v) Члены Совета обеспечивают, чтобы их департаменты и учреждения сотрудничали с Советом и предоставляли Совету такую помощь, информацию и консультации, какие Совет может запросить, в пределах, разрешенных законом.

(vi) Создание и функционирование Совета не должно противоречить существующим полномочиям и обязанностям департаментов и учреждений.

(vii) По вопросам технологической политики и стратегии, касающимся в первую очередь национальной безопасности, Совет координирует свою деятельность с Советом национальной безопасности (СНБ) через заместителя Советника по национальной безопасности по кибернетике и новым технологиям с целью разработки политики и процедур для Совета, которые

уважают обязанности и полномочия СНБ в соответствии с действующим законодательством.

Раздел. 3. Функции Совета. Совет должен:

(a) разрабатывать рекомендации для Президента по вопросам конкурентоспособности технологий США и связанным с ними вопросам, консультировать Президента и оказывать ему помощь в разработке и осуществлении национальной технологической политики и стратегии, а также выполнять другие обязанности, которые Президент может предписать;

(b) осуществлять разработку и надзор Национальной технологической стратегии в соответствии с требованиями раздела 4 настоящего приказа;

(c) выступать форумом для балансирования национальной безопасности, экономических и технологических решений департаментов и агентств США, имеющих отношение к технологическим исследованиям, разработкам, коммерческим интересам и приложениям национальной безопасности;

(d) координировать политику всех департаментов и ведомств США, связанных с конкурентоспособностью США в области критических и новых технологий, и обеспечивать проведение интегрированной и взаимоукрепляющей политики, направленной на поощрение лидерства США и защиту существующих конкурентных преимуществ;

(e) синхронизировать бюджеты и стратегии в консультации с Директором Управления по вопросам управления и бюджета в соответствии с Национальной технологической стратегией.

Раздел. 4. Национальная технологическая стратегия. Политика Соединенных Штатов заключается в сохранении лидерства в критических и новых технологиях, необходимых для национальной безопасности и экономического процветания США. В течение одного года с даты настоящего распоряжения, а также ежегодно после этого Совет представляет Президенту Национальную технологическую стратегию, содержащую следующие элементы:

(a) оценка усилий правительства США по сохранению лидерства США в ключевых новых технологиях и недопущению использования американскими стратегическими конкурентами передовых технологий для получения стратегических военных или экономических преимуществ над Соединенными Штатами;

(b) обзор существующей технологической политики правительства США, включая долгосрочные цели;

(c) анализ технологических тенденций и оценка относительной конкурентоспособности технологических секторов США по отношению к стратегическим конкурентам;

(d) определение секторов, имеющих решающее значение для долгосрочной устойчивости инновационного лидерства США в области проектирования, производства, цепочек поставок и рынков;

e) рекомендации в отношении стимулов внутренней политики для поддержания инновационной экономики и развития конкретных дорогостоящих секторов, необходимых для достижения долгосрочных целей национальной безопасности;

(f) рекомендации в политике защиты руководства США и союзников в критических областях посредством целенаправленного экспортного контроля, проверки инвестиций и контрразведывательной деятельности;

(g) определение приоритетных внутренних областей НИОКР, имеющих решающее значение для национальной безопасности и необходимых для поддержания лидерства США, направление финансирования для заполнения пробелов в фундаментальных и прикладных исследованиях, где отсутствует частный сектор;

(h) рекомендации по программам, направленным на развитие талантов США в ключевых критических и новых технологиях и расширение возможностей федерального правительства по набору и удержанию лиц с навыками по критическим технологиям на федеральной службе;

(i) методы содействия развитию международных партнерств для укрепления внутренней политики, создания новых рынков, участия в совместных исследованиях и создания международной среды, отражающей ценности и защищающей интересы США.

Раздел. 5. Консультативный комитет по конкурентоспособности технологий.

(a) Создание Консультативного комитета по конкурентоспособности технологий (Комитет) для предоставления консультаций и рекомендаций Совету и по вопросам, входящим в сферу компетенции Совета.

(b) В состав Комитета входят помощник Президента по вопросам технологической конкурентоспособности и не более 16 дополнительных членов, назначаемых Президентом. В число дополнительных членов входят выдающиеся лица, не входящие в федеральное правительство. Они должны обладать разнообразным опытом и знаниями в области национальной безопасности, экономической конкурентоспособности, в критических и новых технологиях, имеющих отношение к Национальной технологической стратегии. Помощник Президента по вопросам технологической конкурентоспособности наряду с одним нефедеральным членом Комитета выполняет функции сопредседателя. Члены Комитета несут службу без какой-либо компенсации за свою работу в Комитете, но могут получать путевые расходы, включая суточные вместо прожиточного минимума, как это разрешено законом для лиц, периодически проходящих государственную службу (5 U. S. C. 5701-5707).

(c) Комитет проводит заседания по указанию Сопредседателей Совета и предоставляет консультации или рабочий продукт исключительно для использования Советом при выполнении своих обязанностей в соответствии с настоящим указом.

(d) Административное управление в Административной канцелярии Президента обеспечивает такое финансирование и административную и техническую поддержку, которые могут потребоваться Комитету.

(e) Комитет прекращает свою деятельность через два года с даты принятия настоящего постановления, если оно не продлено Председателем.

Раздел. 6. Общие положения.

(a) Если какое-либо положение настоящего указаа или применение какого-либо положения будет признано недействительным, остальная часть настоящего указа и другие несходные применения такого положения не будут затронуты.

(b) Настоящий указ не предназначен и не создает каких-либо прав или выгод, материальных или процессуальных, подлежащих исполнению по закону или по справедливости любой стороной в отношении Соединенных Штатов, их департаментов, агентств или организаций, их должностных лиц, служащих или агентов, или любого другого лица.

(c) Ничто в настоящем указе не должно толковаться как наносящее ущерб или затрагивающее иным образом:

(i) полномочия, предоставленные законом исполнительному департаменту или учреждению или его руководителю;

ii) функции Директора Управления по вопросам управления и бюджета, связанные с бюджетными, административными или законодательными предложениями.

(d) настоящий указ выполняется в соответствии с применяемым законодательством и при условии наличия ассигнований.

Глава 10: Конкурс талантов

План действий

Соединенные Штаты должны резко инвестировать в свои таланты в области искусственного интеллекта (ИИ), чтобы оставаться на переднем плане по ИИ сейчас и в будущем. Крайне важно, чтобы Соединенные Штаты стратегически инвестировали в науку, технику, инженерное и математическое образование (STEM) на всех уровнях и улучшали иммиграционную систему, чтобы позволить большему количеству талантов ИИ въезжать и оставаться в Соединенных Штатах. Таким образом, этот План действий состоит из двух

широких категорий рекомендаций по укреплению системы талантов США: система образования США и иммиграция.

Трубопровод талантов: Система образования США

Инвестиции в STEM-образование являются необходимой частью повышения американской национальной мощи и укрепления национальной безопасности. Это требует от Соединенных Штатов реформировать свою систему образования, чтобы выпускать как можно более качественных выпускников.

Рекомендация: Принять Новый Закон об образовании в области национальной обороны

В ответ на советский запуск спутника в 1957 году Соединенные Штаты приняли Закон об образовании в области национальной обороны (NDEA) в 1958 году, чтобы расширить лидерство США в области образования и инноваций.1 NDEA пропагандировал важность науки, математики и иностранных языков для студентов, разрешив более 1 миллиарда долларов на сокращение студенческих кредитов, финансирование образования на всех уровнях и финансирование аспирантур. Многие студенты смогли поступить в колледж из-за этого законопроекта; В 1960 году колледж посещали 3,6 миллиона студентов, а к 1970 году-уже 7,5 миллиона. Этот закон помог Америке выиграть Космическую гонку и ускорил нашу способность к инновациям, и считается одним из самых успешных законодательных актов в области образования в истории США.

Теперь настало время для нового NDEA, что значительно увеличит число американцев с высшим образованием, расширит число учителей математики и естественных наук, чтобы удовлетворить спрос на систему К-12 послевоенного бэби-бума и будет сосредоточена на оборонно-ориентированных областях, особенно на нехватке математиков. Влияние федеральных расходов на высшее образование сегодня является отголоском инвестиций, сделанных в конце 1950-х годов администрацией Эйзенхауэра. Соединенные Штаты нуждаются во втором NDEA (NDEA II) для того, чтобы устранить нынешний разрыв в

цифровых талантах и предотвратить отставание Соединенных Штатов в гонке за талантами в области искусственного интеллекта и STEM.

Действия для Конгресса:

• Увеличить финансирование внешкольных программ, ориентированных на STEM и искусственный интеллект;

Программы послешкольного обучения, ориентированные на STEM и AI, открывают студентам доступ к программам, связанным со STEM и AI за пределами обычных школьных часов. Продолжительность учебного дня ограничивает возможности учителей охватить множество тем. Американские учащиеся начальной школы в течение учебного дня в среднем изучают 20 минут естественных наук и 60 минут математики.3 Учитывая тот короткий промежуток времени, который учителя могут тратить на STEM в своих классах, некоторые школьные округа начали предлагать внеклассные программы, которые знакомят учащихся со STEM в менее структурированной среде. Больше времени, потраченного на изучение тем STEM, помогает студентам набирать тестовые баллы, а для тех, кто недостаточно представлен в областях STEM, федеральное финансирование внешкольных программ повысит доступность к качественным образовательным инструментам. Ассигнования на внеклассные программы должны благоприятствовать заявкам, которые совместно подаются местным образовательным учреждением и общинной организацией или другой государственной или частной организацией в качестве способа покрытия расходов и поощрения участия общин.

• Увеличить финансирование летних учебных программ, ориентированных на STEM и искусственный интеллект.

Летние учебные программы, ориентированные на STEM и AI, будут поощрять студентов участвовать в деятельности STEM и AI в те месяцы, когда студенты, как правило, не задействованы и испытывают потерю обучения. Закон об общинных учебных центрах 21-го века является примером программы, которая финансирует «возможности академического обогащения во внеклассное время для детей, особенно учащихся, посещающих школы с

высоким уровнем бедности и низкой успеваемостью», и продемонстрировала доказанные положительные результаты. Как и инициатива по внешкольному обучению, приоритет должен отдаваться тем заявкам, которые подаются совместно местным образовательным учреждением и общинной организацией или другим государственным или частным учреждением.

• Выделять средства на набор, удержание и обучение преподавателей K-12 STEM

Учителя являются неотъемлемой частью процесса обучения по предметам STEM. Одно из неравенств – это отсутствие учителей, обладающих необходимыми знаниями в области STEM. Фактические данные свидетельствуют о том, что подготовка STEM для нынешних учителей является спорадической и неэффективной в удовлетворении конкретных потребностей отдельных учащихся. Кроме того, трудно набирать высококачественных учителей K-12 с опытом и навыками STEM. Это особенно важно, поскольку учителя являются одним из наиболее влиятельных аспектов школы, оказывая в два-три раза большее влияние, чем другие компоненты, такие как лидерство и школьные услуги. Поскольку мир продолжает интегрировать технологии в образование, учителей необходимо учить использовать эту технологию, а также технологию обучения учащихся критическим основам и основным функциям, которые с ней связаны.8 При этом предпочтение следует отдавать курсам повышения квалификации, которые учитывают требования непрерывного образования к аттестации учителей.

• Направлять и финансировать Национальный научный фонд для создания стипендий и стипендий STEM

Мы рекомендуем NSF создать 25 000 стипендий STEM для студентов, 5000 стипендий STEM PhD и 500 постдокторских должностей в течение пяти лет, чтобы увеличить количество и качество практиков STEM и AI, которые выйдут на рынок труда через несколько лет. Рост национального кадрового резерва STEM в востребованных областях требует конвейера студентов, которые бы изучали соответствующие курсовые работы STEM в течение своей

карьеры бакалавра. В период с 2000 по 2017 год доля полученных степеней бакалавра STEM – в процентах от общего числа степеней бакалавра, полученных в США, – выросла с 32% до 35%. Самый резкий рост в последнее время наблюдался среди специальностей информатики и инженерии. В частности, для ИИ степень в области когнитивных наук или компьютерных наук с концентрацией в ИИ или машинном обучении (мл) может проложить путь для будущей карьеры в области исследований ии или практики. ИИ редко предлагается в качестве специальности на уровне бакалавриата. Вместо этого университеты предлагают отдельные курсы, последовательность курсов ИИ или возможность изучать техническую специальность с концентрацией на ИИ. До тех пор, пока специальность в области ИИ не станет более универсальной в университетах США, стипендии STEM увеличат число людей, обладающих навыками, необходимыми для работы над ИИ.

Стипендиаты должны получать полное обучение, комнату для проживания и питание. Студенты должны получать стипендию в размере 40 000 долларов в год, а выпускники должны получать стипендию в размере 70 000 долларов в год. В сочетании с постдокторскими должностями это приведет к тому, что общие расходы составят 7,2 миллиарда долларов в течение пяти лет.

Действия для Департамента образования:

• Добавить элементы вычислительного мышления и статистики в тестирование студентов

Вычислительное мышление и статистика жизненно важны для студентов, чтобы понять, как работает ИИ. Как междисциплинарные области, использование вычислительного мышления и статистики в рамках ИИ может быть найдено на всех этапах открытия, от разработки и планирования исследований до оценки результатов. Критическое мышление наряду с решением проблем являются жизненно важными навыками, которым обучают в статистике. К сожалению, большинство средних школ в Америке не требуют тестирования навыков, связанных с вычислительным мышлением, для получения диплома. Нет никакого способа всесторонне измерить общие

способности или склонность студентов США к навыкам, связанным с вычислительным мышлением и статистикой. Студентов учат тому, что необходимо для сдачи экзаменов. По сравнению с другими странами, многие из которых имеют статистику в своей учебной программе, Соединенные Штаты занимают низкое место по математике. Включив предметы, имеющие решающее значение для вычислительного мышления и статистики в стандартизированное тестирование на государственном уровне, Соединенные Штаты смогут лучше понять возможности учащихся и работать над внедрением учебных программ и уроков, в большей степени ориентированных на вычислительное мышление и статистику для обеспечения их успехов.

Рекомендация: Требовать статистику и принципы информатики в средней школе

Действия для законодательных органов штатов:

• Требовать наличия статистики и принципов информатики в качестве обязательного курса в средней школе. Многие фундаментальные понятия в ИИ, мл и их подполях являются скрытой прикладной статистикой. Используемые методы и алгоритмы в значительной степени основаны на статистических методах, таких как кластерный анализ и выбор моделей. Статистика и принципы информатики необходимы для подготовки студентов к курсам ИИ, концентрациям и стажировкам. Предоставление обучения статистике, начиная со средней школы, позволит лучше подготовить студентов к всё более продвинутым аналитическим методам, востребованным для карьеры в области искусственного интеллекта и STEM. Точно так же в настоящее время только 47% американских средних школ предлагают курсовые работы по информатике. Это намного выше, чем всего десять лет назад, благодаря национальным инициативам, но это все ещё оставляет многие средние школы без образования в области компьютерных наук. Кроме того, принятие было частичным, и глубина учебной программы сильно варьировалась. Поэтому необходимы действия государства.

• Сами по себе ни статистика, ни информатика не являются достаточными для обучения студентов понятиям, необходимым для понимания ИИ. Наличие того и другого позволяет студентам испытать критические основы, которые должны быть охвачены на ранней стадии, чтобы подготовить студентов к технологической карьере. Простая математика, такая как базовая вероятность и суммирование числовых данных, применяет концепции статистики и информатики.

Конвейер талантов: Иммиграция

Иммиграционная реформа крайне необходима для укрепления американского потока талантов, особенно учитывая значительные преимущества, которые Соединенные Штаты получают благодаря высококвалифицированной иммиграции. Поэтому Соединенные Штаты должны проводить реформы, направленные на ускорение иммиграции высококвалифицированных специалистов и удержание иностранных студентов в Соединенных Штатах.

Следующие рекомендации призваны помочь Соединенным Штатам возглавить мировую разработку и внедрение ИИ, получив решающее большинство критического и ограниченного ресурса: таланта ИИ. Эти рекомендации улучшат способность Соединенных Штатов привлекать таланты в Соединенные Штаты и, что не менее важно, подальше от конкурирующих стран.

Соединенные Штаты должны предпринять смелые шаги, чтобы обеспечить себе победу в конкурсе международных талантов на долгие годы. Такие шаги должны обеспечить привлечение нашей иммиграционной системой студентов, технических экспертов и предпринимателей; обеспечить стабильность, пока они продолжают вносить свой вклад в американскую экономику и исследовательскую среду; и удерживала студентов, предпринимателей и экспертов, а не отправляла их домой или в конкурирующие страны. Лучший способ достичь этих целей и послать четкий сигнал ИИ и STEM-талантам по всему миру – это принять Закон об

иммиграции национальной безопасности, который специально помогает STEM-талантам оставаться в Соединенных Штатах, снижает общее бремя процесса получения гражданства и создаёт конкретные пути для предпринимателей.

Рекомендация: Принять Закон об иммиграции национальной безопасности

1) Выдавать Грин-карты всем студентам, получившим степень доктора философии STEM в Аккредитованных американских университетах

Это дало бы невероятно ясный сигнал талантливым молодым людям во всём мире, что они приветствуются в Соединенных Штатах, и облегчило бы их переход к американскому гражданству. Это очень агрессивный маневр, чтобы получить большую долю мирового таланта STEM.

Такое предложение является смелым по общему признанию, но преимущества привлечения проверенных талантов высшего уровня перевешивают риски. Необходимы смелые меры, чтобы сохранить преимущества Америки в области STEM сегодня и гарантировать, что мы превзойдем конкурентов в будущем. Немногие другие предложения достаточно значительны, чтобы кардинально изменить конкуренцию за таланты или поставить Китай перед дилеммой на внутреннем фронте. Примечательно также, что подобные предложения в прошлом получали двухпартийную поддержку.

Действия для Конгресса:

• Внести поправку в пункт 8 U. S. C. 1151(b)(1) о предоставлении законного постоянного места жительства любому иностранному гражданину, который:

Является выпускником аккредитованного высшего учебного заведения Соединенных Штатов с докторской степенью в области науки, техники, инженерии или математики в резидентной или смешанной резидентной и дистанционной программе;

Имеет предложение о работе в области, связанной с наукой, техникой, инженерией или математикой;

Не представляет угрозы национальной безопасности Соединенных Штатов.

• Проверка интересов национальной безопасности должна осуществляться ФБР и разведывательным сообществом.

• Выпускники, получившие законное постоянное место жительства в рамках этой программы, не должны засчитываться в общий лимит грин-карт или лимит грин-карт страны происхождения.

2) Удвоить количество Грин-карт, основанных на трудоустройстве

Независимо от того, нацелены ли Соединенные Штаты на достижение доминирования ИИ, рост валового внутреннего продукта (ВВП), стимулирование роста рабочих мест, сокращение государственного дефицита или повышение платежеспособности американской программы социального обеспечения, самое простое решение остается тем же: увеличить число высококвалифицированных постоянных жителей. При нынешней системе грин-карт, основанных на трудоустройстве, не хватает 140 000 в год, из которых менее половины достаётся основному работнику. В результате многие высококвалифицированные работники не могут получить постоянное место жительства и не могут переводить работу или вести переговоры с работодателями эффективно и находятся на положении домашней прислуги. Если им недоплачивают, они не могут уйти с работы или договориться о более высокой зарплате, не рискуя лишиться спонсорской помощи работодателя по грин-карте или даже уволиться и принудительно уехать из Соединенных Штатов. Это снижает привлекательность присоединения к американской рабочей силе.

Система H-1B также проблематична для большинства работодателей, поскольку ежегодно проводится «лотерея» из 85 000 виз (из которых 20 000 зарезервированы для обладателей высших степеней из университетов США). Чтобы сократить отставание высококвалифицированных работников, Соединенным Штатам следует удвоить число грин-карт, основанных на трудоустройстве, с акцентом на постоянное проживание в областях, связанных

с STEM и ИИ. Если бы это было проще для США. работодатели, спонсирующие глобальные таланты для получения грин-карты в отличие от визы H-1B, программа H-1B могла бы тогда выполнять свою первоначальную предназначенную функцию в качестве средства для действительно временных потребностей в высококвалифицированной работе.

Действия для Конгресса:

• Изменить 8 U. S. C. 1151(d)(1)(A), изменив «140 000 плюс» на «280 000 плюс

3) Создать визу предпринимателя

Иностранные докторанты с большей вероятностью захотят основать компанию или стать сотрудником стартапа, чем их соотечественники, но на практике они с меньшей вероятностью пойдут по этому пути. Одна из причин – ограничения визовой системы H-1B.23 Точно так же предприниматели-иммигранты, не имеющие капитала для использования маршрута EB-5 для постоянного проживания, вынуждены использовать другие визы, предназначенные для ученых и работников существующих компаний, а не для предпринимателей.24 Все эти проблемы делают Соединенные Штаты менее привлекательными для международных талантов и, что не менее важно, снижают способность стартапов и других небольших компаний, основного источника новых рабочих мест для американцев, нанимать высококвалифицированных иммигрантов, которые, как было показано, повышают шансы на успех бизнеса.

Действия для Конгресса:

• Создайте визу предпринимателя. Эта виза должна служить альтернативой визам, спонсируемым сотрудниками, инвесторами или студентами, и вместо этого должна быть нацелена на перспективных потенциальных основателей. Законодательство должно:

Определить иностранца как предпринимателя, организация и ведение бизнеса которого принесло бы значительную общественную пользу

Соединенным Штатам, если бы ему было разрешено остаться в стране в течение ограниченного испытательного срока для развития компании.

Расставьте приоритеты предпринимателям, работающим в высокоприоритетных областях, таких как ИИ, или в областях, использующих ИИ для других применений, таких как сельское хозяйство. Национальный научный фонд должен обновлять перечень приоритетных направлений каждые три года.

Используйте захват капитала в качестве критерия отбора предпринимателей.

Подчеркните создание рабочих мест для американцев, потенциально подчёркивая недостаточно обслуживаемые регионы или районы с высокой безработицей в качестве основного фактора при оценке значительных общественных выгод.

4) Создать новую и разрушительную технологическую визу

Новая неиммиграционная виза, предназначенная для привлечения лучших технологических талантов в критических областях, позволит университетам и предприятиям, работающим над ИИ и другими новыми технологиями, получить доступ к большему пулу талантов, необходимых для создания передовых исследований. Она также будет более гибко реагировать на требования рынка труда по мере появления новых технологий. Результатом будет «оживление исследовательской экосистемы нашей страны, расширение возможностей инновационной экономики нашей страны и обеспечение Соединенным Штатам статуса мировой сверхдержавы в ближайшие десятилетия.»

Действия для Конгресса:

• Создать новую и разрушительную технологическую визу, которая:

Требует от Национального научного фонда каждые три года выявлять новые критические и прорывные технологии;

Предоставляет возможность применения в соответствующих областях студентам, исследователям, предпринимателям и технологам;

Не включает в себя новые и прорывные технологии держателей виз в любой другой категории виз.

Рекомендация: Расширить сферу применения «Экстраординарных» талантов, чтобы сделать визу O-1 Более доступной и подчеркнуть талант ИИ.

Временная рабочая виза O-1 предназначена для людей с экстраординарными способностями или достижениями.26 Визы O-1 действительны в течение трех лет и могут продлеваться ежегодно неограниченное количество раз. Также нет ограничений на количество выдаваемых виз в год. В настоящее время ежегодно выдается от 15 000 до 18 000 новых виз O-1.27 По этим причинам виза O-1, как правило, является более гибкой из категории виз, чем виза H-1B, которая, за некоторыми исключениями, ограничена по продолжительности и количеству виз.

Хотя визы O-1 дают много преимуществ, они плохо подходят для многих высококвалифицированных работников из-за неопределённости их критериев и административного бремени процесса подачи заявления и вынесения судебного решения. Судьи определяют приемлемость кандидата путем субъективной оценки того, получили ли кандидаты национально признанные премии, были ли они опубликованы в крупных изданиях, выполнили ли они оригинальную работу, имеющую большое значение, и соответствуют ли они другим аналогичным критериям. Это в значительной степени соответствует таким академическим критериям, как публикации в крупных изданиях для науки и техники, и не очень хорошо подходит для людей, которые преуспевают в промышленности.

Действия для Службы гражданства и иммиграции США (USCIS):

• Издать новое руководство с чёткими и широкими стандартами для регулирующих критериев, исходя из того, что считается крупным выходом, признанной на национальном уровне премией или оригинальной работой.

Например, если публикация в пяти ведущих академических журналах в области науки считается крупным изданием, многие выпускники PhD, скорее всего, будут претендовать на это.

• Инициировать регулирующий процесс для снижения порога для получения визы O-1, например, путем сокращения числа критериев, которые заявитель должен выполнить.

Нынешний стандарт – это три из восьми критериев.29

• Расширить критерии, чтобы лучше принимать неакадемические достижения ИИ и STEM.

Например, некоторые инженеры высшего уровня не получили степень бакалавра и не опубликовали крупных работ, вместо этого сосредоточившись на разработке и монетизации передовых технологий в частном секторе. Новые критерии должны сделать визы O-1 более доступными для этой демографической группы.

Рекомендация: Внедрить и рекламировать Правило международного предпринимателя

Правило международного предпринимателя (IER) позволяет USCIS предоставлять период разрешенного пребывания международным предпринимателям, которые демонстрируют, что «их пребывание в Соединенных Штатах принесёт значительную общественную выгоду через их деловое предприятие».30 IER будет относительно легко реализовываться Исполнительной властью и более непосредственно связан с созданием рабочих мест, чем большинство других иммиграционных предложений, что делает его более полезным для большинства американцев.

Действия для президента:

• Немедленные действия исполнительной власти могут объявить о намерении администрации использовать IER для стимулирования предпринимательства иммигрантов, создания рабочих мест для американцев и экономического роста.

Действия для USCIS:

• Объявите, что USCIS будет отдавать приоритет предпринимателям, работающим в высокоприоритетных областях STEM, таких как ИИ или в областях, использующих ИИ для применения, например, в сельском хозяйстве.

• Использовать объём капитала в качестве критерия отбора предпринимателей.

• Подчёркивать создание рабочих мест для американцев в недостаточно обслуживаемых регионах или районах с высокой безработицей в качестве основного фактора при оценке возможностей значимых общественных выгод.

Рекомендация: Расширить и уточнить переносимость рабочих мест для высококвалифицированных работников

Министерство внутренней безопасности (DHS) опубликовало в ноябре 2016 года окончательное правило, которое внесло ряд реформ в целях улучшения программ временных рабочих виз, включая некоторую меру облегчения для работников, привязанных к работодателю, спонсирующему их ходатайство о грин-карте в течение потенциально десятилетнего периода ожидания. Это правило позволяет работникам, имеющим визы H-1B, O-1 и другие временные рабочие визы, получать разрешения на работу на открытом рынке, на один год, с возможностью продления при наличии непреодолимых обстоятельств. К числу непреодолимых обстоятельств относятся:

• Серьезное заболевание или инвалидность, с которыми сталкивается работник или его иждивенцы,

• Наказание работодателя в отношении работника,

• Другой существенный вред, причиненный работнику,

• Значительное нарушение работы работодателя.32

Критерии принуждения слишком ограничены и неоднозначны. Расширение возможностей обладателей виз в получении разрешения на работу позволило бы повысить уровень предпринимательской активности, более тесно взаимодействовать с новыми работодателями и вести переговоры о компенсации на равных условиях с домашними работниками.

Действия для USCIS:

• Разъяснить, когда высококвалифицированным неиммиграционным работникам разрешается менять работу или работодателей;

• Повышать гибкость работы в условиях, когда работодатель либо отзывает свое ходатайство о H1B, либо приобретается, сокращается или выходит из бизнеса;

• Повышать гибкость для работников H-1B, ищущих другую работу H-1B.

Рекомендация: Вернуть Грин-карты, потерянные из-за бюрократической ошибки

Конгресс устанавливает ежегодные ограничения на количество грин-карт, которые могут быть выданы некоторым семейным иммигрантам (226 000) и иммигрантам, работающим по найму (140 000). 33 Поскольку федеральные агентства не хотят превышать годовой лимит грин-карт, они обычно выпускают меньше грин-карт, чем им разрешено. Из-за этой тенденции по состоянию на 2009 год федеральное правительство выпустило не более 326 000 грин-карт.34 Сегодня это число, скорее всего, выше, но DHS не опубликовала обновлённую статистику.

Действия для Департаментов внутренней безопасности и государства:

• Опубликовать ежегодный отчет о количестве грин-карт, потерянных из-за бюрократической ошибки.

• Рассмотреть вопрос о том, можно ли использовать имеющиеся органы власти для:

Выпуска потерянных грин-карт в следующем году без учета ограничений по грин-картам.

Отдачи приоритета высококвалифицированным иммигрантам, которые ждали дольше всех, а затем высококвалифицированным иммигрантам с длительным прогнозируемым временем ожидания.

• Если имеющейся власти недостаточно, вступите в контакт с Конгрессом, чтобы вернуть грин-карты, потерянные из-за бюрократической ошибки, с помощью специального законодательства.

Соединенные Штаты остаются мировым лидером в области искусственного интеллекта (ИИ), однако тенденции внутри Соединенных

Штатов указывают на скрытые слабые стороны. Федеральное правительство несёт ответственность за обеспечение стратегического направления и долгосрочных ресурсов для укрепления национальной основы инноваций в области искусственного интеллекта. Соединенные Штаты через государственное управление и в партнерстве с промышленностью и научными кругами должны увеличить разнообразие, конкурентоспособность и доступность своей инновационной среды ИИ, чтобы обеспечить постоянное лидерство.

Рекомендация: Масштабировать и координировать федеральное финансирование НИОКР в области искусственного интеллекта

Соединенные Штаты должны укрепить фундамент технического лидерства в области ИИ, приняв смелый, устойчивый федеральный толчок к инвестициям в НИОКР ИИ, чтобы способствовать общенациональному ландшафту инноваций ИИ и стимулировать прорывы в следующем поколении технологий ИИ, создав Национальный технологический фонд, финансируя НИОКР ИИ на смешанных уровнях, создавая дополнительные национальные научно-исследовательские институты ИИ и делая большие ставки на таланты и инновационные идеи.

После успешного запуска Россией спутника в 1957 году Конгресс сделал значительные инвестиции в Национальный научный фонд (NSF), чтобы поддержать лидерство США в науке и технике. С тех пор NSF поддерживает исследования на всех рубежах науки и техники, финансируя усилия, которые способствовали развитию Интернета, смартфонов и аддитивного производства. Однако в сегодняшней обострённой геополитической технологической конкуренции необходимы еще более смелые действия, чтобы выполнить обещание новых и разрушительных технологий, таких как ИИ, стимулировать инновации США в национальных интересах и обеспечить наше экономическое будущее.

Комиссия рекомендует создать Национальный технологический фонд (НТФ) в качестве независимого федерального агентства и дочерней

организации NSF, чтобы обеспечить средства для более активного продвижения науки в инженерное дело и масштабирования инновационных идей в реальность. Для этого потребуется организация, структурированная таким образом, чтобы принимать более высокие уровни риска и иметь возможность делать большие ставки на инновационные идеи и людей. Это также требует акцента на переходе технологии из лаборатории на рынок.

* Представление текущих топ-10 федеральных спонсоров исследований и разработок в области ИИ, не связанных с обороной.

В нынешнем федеральном положении в области НИОКР отсутствует организация, обеспечивающая уровень инвестиций и направленность прикладных исследований и технологических разработок, соизмеримых с выгодой, которую технологические прорывы могут принести экономике, обществу и национальной безопасности США. В отличие от фундаментальной науки, развитие технологий представляет собой более дорогостоящее начинание,3 требующее поддержки разнообразной базы исследователей и разработчиков, включая партнёров из частного сектора, и предполагает регулярное принятие рисков. Агентство перспективных оборонных исследовательских проектов (DARPA) делает это эффективно, ориентируясь на конкретные цели национальную безопасности, в первую очередь, с помощью предписанного программного подхода.

НТФ будет стимулировать технологический прогресс на национальном уровне, сосредоточив внимание на создании ценности на промежуточных уровнях технической зрелости,4 приоритизации концепций, основанных на использовании, создании инфраструктуры для экспериментов и испытаний и поддержке коммерциализации успешных результатов. Он будет работать в тесном сотрудничестве с NSF, DARPA и другими межведомственными партнёрами для укрепления инвестиций в отечественную науку и технику (S&T), обеспечивая топливо для разработки и доставки ИИ и других технологий, от которых зависит будущий экономический прогресс и преимущества национальной безопасности.

Чтобы обеспечить уровень внимания к передовым технологиям, имеющим стратегическое значение, НТФ должна сосредоточить усилия вокруг набора регулярно обновляемых приоритетных областей исследований, которые Комиссия определила как технологии, стратегически важные для национальной конкурентоспособности США5:

1. Искусственный интеллект
2. Биотехнологии
3. Квантовые вычисления
4. Полупроводники и современное оборудование
5. Робототехника и автономия
6. 5G и расширенные сети
7. Передовое производство
8. Энергетические технологии

Мы не недооцениваем проблему создания нового института, но рассматриваем ее как стратегический императив. НТФ представляет собой долгосрочную инвестицию в потенциал Америки, связанный с лидерством в области ИИ и других разрушительных технологий и применением этих технологий для достижения общественной значимости. Это обеспечит доступ к ресурсам и инструментам, способствующим росту в национальной культуре числа экспериментов и изобретений с использованием новых технологий.

Учитывая необходимость укрепления критичной целостности национального ландшафта, НТФ не должен снижать уровень ассигнований на НСФ, DARPA или существующие федеральные достижения в области НИОКР. Скорее, НСФ должен выступить одним из инструментом, способствующим укреплению института непреходящей критической важности и усиливающим федеральную поддержку технологических НИОКР по существующим каналам.

Действия для Конгресса:

• Санкционировать и обеспечить надлежащее финансирование для поддержки создания НТФ

Чтобы способствовать предполагаемому расширению технологических достижений США, федеральные инвестиции в НТФ должны постепенно

увеличиваться с 2022 по 2026 финансовый год при конечном расчётном операционном бюджете в 20 миллиардов долларов в год.

Дополнительные средства на оборудование, необходимое для создания Фонда и оцениваемое примерно в 30 миллионов долларов, должны выделяться, начиная с 2022 финансового года.

Членов Национального технологического совета следует назначать Президентом в целях обеспечения политического руководства НТФ, контроля за основными инициативами Фонда и для того, чтобы основные направления его исследований обновлялись с учётом технологических тенденций. Директивы и действия Совета должны основываться на Национальной технологической стратегии, предложенной Комиссией, и, при необходимости, координироваться с Советом по конкурентоспособности технологий, отдельно рекомендуемых в настоящем докладе.

Директор и заместитель директора, назначаемые Президентом, должны координировать программирование в дирекциях Фонда и совместно с внешними организациями.

НТФ следует наделить полномочиями по реализации портфеля обязанностей:

Распределять финансирование через гранты, соглашения о сотрудничестве и контракты, заключаемые в рамках приемлемых для риска конкурентных процессов между академическими и частными исследователями, некоммерческими организациями и консорциумами.

Управлять компонентом его финансирования через инновационное подразделение по образцу DARPA, в котором независимые руководители программ будут финансировать предложения как от промышленных кругов, так и от академических для продвижения решений перспективных исследовательских вопросов.

Содействовать передаче технологических достижений правительству, а также коммерческому сектору.

Проводить призовые конкурсы, чтобы катализировать исследования вокруг важных проблем технологических вызовов.

Управлять национальными технологическими ресурсами и инфраструктурой, демократизирующих способность создавать, тестировать и экспериментировать.

Вносить свой вклад в успех региональных инновационных кластеров, предусмотренных Комиссией, участвуя в предлагаемой офисом технологической программе и поддерживая связь с промышленностью в технологических исследовательских центрах.

Вносить вклад в международное сотрудничество в области НИОКР и вести диалоги по установлению стандартов, укрепляющих стратегическое партнерство США.

Компонент: Увеличить федеральное финансирование уровней компаундирования данных ПВО и уровней, не связанных с обороной, и определить приоритетность ключевых областей ПВО

Исследования – это стержень глобального лидерства Америки в области ИИ. Однако нынешнего федерального финансирования недостаточно для удовлетворения роста отрасли, не говоря уже о поддержке ее дальнейшего расширения. Предлагаемый администрацией Трампа бюджет на исследования и разработки в области ИИ, не связанные с обороной, в 2021 финансовом году составил примерно 1,5 миллиарда долларов, увеличившись с 1 миллиарда долларов, потраченных в 2020 финансовом году. Далее, опираясь на эти инвестиции, Конгресс включил Закон о Национальной инициативе ИИ 2020 года в Закон о национальной обороне на 2021 финансовый год, который создает структуру для более стратегического подхода к использованию ИИ и включает разрешение на дополнительные инвестиции в ИИ в NSF, Министерстве энергетики (DoE), Национальном институте стандартов и технологий (NIST) и Национальном управлении океанических и атмосферных исследований (NOAA).

Закон о национальной инициативе в области ИИ 2020 года

• Создал орган исполнительной власти в рамках Управления научно-технической политики для координации федеральной поддержки исследований и разработок в области ИИ, образования и профессиональной подготовки, научно-исследовательской инфраструктуры и международного участия в целях достижения национальных приоритетов, определенных в регулярно обновляемом стратегическом плане для ИИ.

• Включил положения о создании Национальной целевой группы по исследованиям ИИ, формализовал усилия Национального научно-исследовательского института ИИ и санкционировал финансирование исследований ИИ в Национальном научном фонде, Национальном институте науки и техники, Министерстве энергетики и Национальном управлении океанических и атмосферных исследований. Правительство должно опираться на эти первые шаги и инвестировать в уровни компаундирования данных ПВО. Федеральное финансирование исследований позволит изменить тенденции, ухудшающие возможности США по лидированию в области ИИ из-за ослабления академических исследований в результате утечки мозгов профессоров и оттока аспирантов в промышленность. Отечественный конвейер талантов ИИ не поспевает за потребностями правительства и промышленности, а технологии отстают от национальных технических и этических стандартов развития. Кроме того, федеральная поддержка может стимулировать применение ИИ в других областях науки и техники, что потенциально может привести к значительной отдаче от инвестиций.

Благодаря постоянным инвестициям федеральная поддержка может служить целостному укреплению исследований и разработок в области ИИ, охватывая целый ряд инициатив, включая поддержку фундаментальных и прикладных исследований, совместную исследовательскую инфраструктуру, сеть институтов ИИ, стипендий и конкурсов. Поток инвестиций через различные агентства создаст динамичную структуру финансирования, ориентированную как на миссию, так и на исследования, уравновесит

поддержание эволюционного прогресса с большими ставками на революционные прорывы и поддержит инновации в академических кругах и частном секторе.

Действия для Конгресса

• Удвоить ежегодное финансирование исследований и разработок в области ИИ, не связанных с обороной, и достичь 32 миллиардов долларов к 2026 финансовому году

Конгресс должен поддерживать увеличение объемов федерального финансирования AIR&D, ежегодно удваивая инвестиции по сравнению с базовым уровнем в 1 миллиард долларов в 2020 финансовом году.

Инвестиции должны быть сделаны через федеральные агентства по финансированию НИОКР, в частности, предлагаемый Национальный технологический фонд, DoE, NSF, Национальные институты здравоохранения (NIH), NIST и Национальное управление по аэронавтике и исследованию космического пространства (NASA).

Значительные средства должны быть выделены на расширение стипендиальных программ. Увеличение финансирования с помощью этих механизмов будет способствовать увеличению числа студентов и аспирантов, обучающихся в областях, связанных с искусственным интеллектом, помогая укрепить академические круги, расширить внутренний канал талантов и обеспечить путь в правительство для технических талантов. Аналогичным образом, карьерные/факультетские стипендии, поддерживающие исследователей в академических кругах, послужат сдерживанию оттока исследователей в промышленность и инвестированию в лучшие таланты для реализации больших идей.

• Взять на себя обязательство тратить не менее 1% ВВП на НИОКР, финансируемые из федерального бюджета

Чтобы поддерживать сильную инновационную базу в научно-технической сфере, Конгресс должен сочетать конкретные инвестиции в ИИ с общим федеральным обязательством ежегодно финансировать НИОКР на

уровне, достигающем не менее 1% валового внутреннего продукта (ВВП). Это может быть достигнуто за счет устойчивого роста в течение следующих пяти лет со скоростью около 15 миллиардов долларов в год.

Меры для Управления научно - технической политики:

• Сбалансировать Межведомственные Инвестиционные Портфели НИОКР ИИ

Национальная инициатива по ИИ должна координировать федеральные инвестиции в НИОКР в направлении ежегодного удвоения контрольных показателей путем увеличения финансирования исследований, стипендий и создания исследовательской инфраструктуры.

Национальная инициатива по ИИ должна обеспечить рост финансирования между несколькими учреждениями и воплощать в себе портфельный подход для использования разнообразного набора механизмов, ориентированных на целый ряд результатов – продвижение фундаментальной науки, решение конкретных проблемных задач и содействие коммерциализации прорывов.

• Определение приоритетов в важнейших областях исследований ИИ

Инвестиции должны отдавать приоритет тем областям исследований, которые имеют решающее значение для развития технологий искусственного интеллекта, которые будут лежать в основе будущей национальной безопасности и экономического роста, но могут не получить значительных инвестиций для частного сектора, таких как:

Новые направления машинного обучения (мл). К дальнейшим нетрадиционным подходам к контролируемому ОД в неконтролируемой или полуконтролируемой манере, а также к переносу обучения с одной задачи или предметной области на другую.14 Другие направления включают изучение гибридных методов ИИ, которые сочетают ИИ, ориентированный на данные, с различными формами представлений на основе моделей и методологиями вывода для извлечения выгоды из взаимодополняющих сильных сторон.15

Тестирование и оценка, верификация и валидация (TEVV) систем ИИ. Развить лучшее понимание того, как проводить TEVV и создавать сдержки и противовесы во всем жизненном цикле системы ИИ,16 включая усовершенствованные методы исследования, прогнозирования и управления поведением отдельных систем ИИ, для того, чтобы при встраивании в системы систем ИИ их взаимодействие не приводило к неожиданно негативным результатам. Понимать контекстную специфику и ухудшение производительности в новых и невидимых средах.

Крепкий и жизнерадостный мл. Культивировать более надежные методы, способные преодолевать неблагоприятные условия, и продвигать подходы, позволяющие оценивать типы и уровни уязвимости и иммунитета. Решение проблем, связанных с несколькими классами состязательных атак мл, включает в себя справедливые исследования.

Сложные мультиагентные сценарии. Углубить понимание взаимодействующих когорт систем искусственного интеллекта, включая исследования состязательных уязвимостей и смягчений последствий, а также применение теории игр к разнообразным и сложным сценариям.

ИИ для моделирования, симуляции и проектирования. Развивать использование богатых симуляций в качестве источника синтетических данных и сценариев для обучения и тестирования систем ИИ, а также использовать ИИ для решения сложных аналитических задач и служить генеративным двигателем проектирования в научных открытиях и инженерии.

Расширенное понимание сцены. Разработать перцептивные модели, включающие многоисточниковую и мультимодальную информацию для поддержки, расширенной практической осведомленности и понимания в различных динамичных сложных средах и сценариях.

Сохранение личной неприкосновенности. Для обеспечения личной конфиденциальности отдельных лиц обеспечивается защита при сборе и использовании данных для разработки и эксплуатации систем искусственного интеллекта с помощью достижений в области методов анонимности и

технологий по сохранению конфиденциальности, таких как гомоморфное шифрование, дифференциальные методы конфиденциальности и многопартийное федеративное обучение.

Оценка рисков системы ИИ. Расширенные возможности поддержки оценки рисков, включая стандартные методы и метрики для оценки степени аудируемости, прослеживаемости, интерпретируемости, объяснимости и надёжности.

Улучшенное взаимодействие человека и ИИ, объединение в команду. Продвижение понимания объединения людей и ИИ, включая комплементарность человека и ИИ, методы расширения человеческих мыслительных способностей и плавные передачи в системах со смешанной инициативой. Также включает в себя поддержку технологий искусственного интеллекта для лучшего восприятия и понимания человеческих намерений и коммуникаций, включая понимание устной речи, письменного текста и жестов. Прогресс в объединении людей и машин позволит людям взаимодействовать с системами, поддерживающими искусственный интеллект, перейти от нынешней модели взаимодействия, где человек является «оператором», к будущему, в котором люди будут иметь «товарищеские» отношения с машинами.

Автономные системы ИИ. Чтобы повысить способность системы достигать целей независимо или с минимальным контролем со стороны людей-операторов в сложных и непредсказуемых средах.

К более общему ИИ. Исследуйте постоянные сложные проблемы и тайны человеческого интеллекта, включая способность эффективно учиться без контроля; накапливать и применять знания здравого смысла; строить причинно-следственные модели, обеспечивающие надежные объяснения; осуществлять самосознание, оценку и контроль; обобщать и использовать полученные о конкретных задачах знания для профессионализма в других задачах.

Компонент: Утроить число Национальных исследовательских институтов ИИ

NSF выделил гранты для первых Национальных исследовательских институтов ИИ в 2020 году, поддержав семь университетских многоинституциональных консорциумов, организованных вокруг фундаментальных и прикладных областей исследований ИИ-темы, и для которых были определены пути координации с межведомственными и общественными заинтересованными сторонами.17 NSF планирует второй раунд финансирования институтов в 2021 году, координируя поддержку не только с межведомственными партнерами, но и с заинтересованными сторонами частного сектора в целях создания восьми дополнительных институтов.18 Конгресс предпринял шаги по поддержке этой инициативы в рамках Закона о Национальной инициативе в области искусственного интеллекта 2020 года, который формализует эти усилия, предоставляет всем агентствам полномочия по финансовой поддержке создания Национального исследовательского института в области искусственного интеллекта и поручает NSF объединить эти институты в «Сеть лидерства в области искусственного интеллекта».

Расширение этой инициативы создало бы общенациональную сеть инноваций в области ИИ, которая поддерживает широкий спектр исследовательских инициатив в области ИИ – продвижение фундаментальной науки об ИИ, решение проблем в конкретной области и применение ИИ в других областях науки и техники. Их создание увеличило бы возможности для обучения студентов и проведения научных исследований для профессорско-преподавательского состава, исследователей национальных лабораторий и некоммерческих исследовательских организаций; помогло бы расширить сферу деятельности за пределами ведущих частных университетов и региональных технологических центров; и стратегически направить исследования в области, которые могли бы продвинуть науку об ИИ и приложениях ИИ, служащим более широким интересам общества и национальным интересам.

Действия для Конгресса:

• Направить соответствующие средства на расширение сети институтов ИИ.

Конгресс должен направить в НФС соответствующие средства для расширения сети институтов ИИ в три раза в течение последующих трех лет – в идеале это приведет к широкому разнообразию участвующих институтов, регионов и концентраций исследований.

Эти инвестиции охватят 30 дополнительных институтов на общую сумму 600 миллионов долларов для поддержки дополнительных институтов в течение пятилетнего срока действия грантов. Это повлечет за собой ассигнования в размере 200 миллионов долларов в 2022 финансовом году, 2023 финансовом году и 2024 финансовом году.

Меры для Управления научно - технической политики:

• Интеграция сети институтов с национальными инвестициями в инфраструктуру исследований и разработок в области искусственного интеллекта

Национальная инициатива по ИИ должна обеспечить согласование Национальных исследовательских институтов ИИ со стратегическими исследовательскими приоритетами и обеспечить интеграцию с национальной сетью открытых испытательных стендов ИИ и Национальным исследовательским ресурсом ИИ (см. Обсуждение Национальной исследовательской инфраструктуры ИИ ниже).

Компонент: Инвестируйте в таланты, которые изменят сферу деятельности

Лучшие таланты в области ИИ – это дефицитный товар, и инвестиции в таланты имеют потенциал не только для открытия прорывов в науке и применении ИИ, но и для привлечения и удержания лучших талантов в Соединенных Штатах.20 Точно так же инвестиции в исследовательские инициативы, проводимые интегрированными междисциплинарными группами, являются проверенным механизмом для быстрого прорыва, решения сложных проблем и оспаривания существующего статус-кво.

Запуск федерального финансирования премии AI Innovator Award и дополнительной командной премии AI award укрепит способность раздвигать

границы исследований в области ИИ, обеспечивая механизм дополнения текущих инвестиций в нарастающий прогресс ставками на революционные прорывы.

Действия для Конгресса:

• Прямое и финансируемое учреждение премии AI Innovator Award.

Конгресс должен управлять финансированием NSF для создания премии AI Innovator Award, свободно смоделированной по образцу премии NIH Pioneer Award и программы исследователей Медицинского института Говарда Хьюза, чтобы создать гибкий механизм, предоставляющий ведущим исследователям возможность реализации больших идей без предписанных результатов в течение пятилетнего возобновляемого гранта.

В общей сложности около 5,5 млн. долл. США на каждого лауреата в течение пятилетнего срока, эти премии будут полностью покрывать заработную плату и пособия исследователей в их соответствующих учреждениях, а также бюджет исследований, который будет поддерживать оборудование и персонал.

В период своего максимального расцвета программа будет поддерживать 100 исследователей одновременно, достигнув уровня около 125 миллионов долларов годового финансирования на поддержку исследований, с дополнительными средствами, доступными для поддержки основного оборудования.

Подходящими исследователями будут те, кто работая на любом этапе карьеры в американских университетах или исследовательских институтах, обязуется тратить 75% своего времени на исследования.

Отборочный комитет должен обратить внимание на необходимость разнообразия среди награжденных с точки зрения пола, расы, возраста, местоположения и основной области обучения, а также на коммуникативные и лидерские навыки кандидатов.

Конгресс должен разрешить NSF:

Финансировать внешнюю организацию для управления программой.

Ежегодно отбирать от 10 до 20 получателей на пятилетние возобновляемые сроки и проводить отбор через небольшую группу экспертов по ИИ.

Обеспечить отбор инновационных кандидатов с помощью процесса информационно-пропагандистской модели, в рамках которого кандидаты ранжируются в соответствии с максимальными баллами, полученными рецензентами, тем самым отдавая приоритет росту их потенциала.

Проводить ежегодную встречу, на которой все лауреаты представят свою работу, обеспечив место для содержательной обратной связи в рамках обозреваемых циклов и помогая создать сообщество инноваций среди ведущих американских умов в области искусственного интеллекта.

Конгресс должен потребовать от NSF произвести оценку программы после семи лет работы для того, чтобы определить, должна ли она продолжать расширяться или должна продолжить работу с меньшим количеством наград, а также оценить влияние уровня финансирования и срока присуждения премии на исследования, проводимые участниками.

• Прямое и финансируемое учреждение командной премии за исследования в области искусственного интеллекта.

Конгресс должен финансировать NSF для работы с той же внешней организацией, что и премия AI Innovator Award, чтобы создать командную премию для поддержки смелых междисциплинарных исследовательских инициатив, которые применяют ИИ для решения сложных проблем или проводят фундаментальные исследования по его использованию.

Программа должна начинаться с годового бюджета в размере 50 миллионов долларов, а к пятому году поддержка её функционирования должно устойчиво увеличиться до 250 миллионов долларов годового бюджета.

Конгресс должен уполномочить НФС:

Финансировать внешнюю организацию для администрирования программы.

Отбирать от пяти до 10 команд ежегодно на невозобновляемые пятилетние сроки, присуждая от 4 до 10 миллионов долларов в год в течение пятилетнего срока действия премии.

Рекомендация: Расширение доступа к ресурсам ИИ через Национальную исследовательскую инфраструктуру ИИ

Если не решить проблему, растущий разрыв между «имущими» и «неимущими» в области исследований и разработок в области ИИ приведёт к деградации долгосрочных исследовательских и учебных функций, выполняемых США. Университеты ограничивают возможности малого бизнеса по внедрению инноваций и усугубляют отсутствие разнообразия в этой области.30 Хотя развитие за последние пять лет резко расширило доступ к базовым инструментам мл и облачным вычислениям, прогресс в области передовых подходов к ИИ требует значительных объёмов данных и вычислительных мощностей, дорогостоящей инфраструктуры, а также значительного аппаратного и программного обеспечения.

Соединённые Штаты должны способствовать созданию ведущей в мире среды для инноваций в области ИИ посредством демократизации доступа к исследованиям и разработкам в области ИИ, которая поддерживает более справедливый рост области и расширение экспертных знаний в области ИИ по всей стране; позволяет применять ИИ в широком спектре областей науки и техники, коммерческом секторе и секторе государственных услуг; и подпитывает следующие волны инноваций.

Компонент: Запуск Национального исследовательского ресурса по ИИ

После всплеска глубокого обучения в 2012 году и сопутствующего его росту использования специализированного оборудования для вычислений ИИ возникло то, что некоторые называют «вычислительным разрывом»– неравенство в доступе между крупными технологическими компаниями и элитными университетами и средними школами, а среди университетов более низкого уровня – в доступе к ресурсам, необходимым для передовых исследований ИИ. Было обнаружено, что наличие и тип вычислительных

ресурсов оказывают равное «чрезмерное» влияние как на направление исследований, проводимых исследователями, так и на доминирование хорошо оснащенных фирм при смещении общего направления исследований ИИ в сторону прикладных, «узких « возможностей ИИ.

Чтобы преодолеть вычислительный разрыв федеральное правительство должно создать Национальный исследовательский ресурс по ИИ (NAIRR) для предоставления проверенным исследователям и студентам доступа к вычислительным ресурсам совместно с готовыми к ИИ правительственными и неправительственными наборами данных, образовательными инструментами и пользовательской поддержкой. Эта инфраструктура должна использовать государственно-частное партнерство, передовые технологии частного сектора и опираться на существующие правительственные достижения во избежание высоких затрат на запуск государственного центра обработки данных. Конгресс сделал первый шаг в рамках Закона о национальной обороне на 2021 финансовый год, реализовав компонент предыдущей рекомендации Комиссии о создании целевой группы по разработке дорожной карты для NAIRR.35 Результаты этих усилий будут представлены Конгрессу через 18 месяцев после назначения членов целевой группы.

Действия для Конгресса:

• Санкционировать выделение 30 миллионов долларов на реализацию дорожной карты NAIRR

Конгресс должен санкционировать и выделить соответствующие средства для немедленной реализации дорожной карты, разработанной Военно-воздушной целевой группой.

Этот ресурс должен поддерживаться на первоначальном уровне в размере 30 млн. долл. США в год, увеличиваться за счет взносов партнёров из частного сектора и расширяться по мере его становления и привлечения пользователей.

Финансирование будет поддерживать кадровое обеспечение программы и облачные ресурсы, дополненные за счет государственно-частного партнерства. Сотрудники будут отвечать за поддержание и совершенствование

архитектурного решения, курирование наборов данных, создание интерфейсов и инструментов, а также оказание поддержки исследователям.

Компонент: Создание Сети национальных испытательных стендов ИИ для обслуживания академических и отраслевых исследовательских сообществ

Спонсируемая различными федеральными агентствами, сеть национальных испытательных стендов ИИ обеспечит реальные, предметно-ориентированные ресурсы, открытые для академических, деловых и правительственных исследовательских сообществ, чтобы стимулировать фундаментальные и прикладные исследования для решения сложных проблем и разработки надежных, пригодных к использованию систем ИИ, готовых к коммерциализации (например, испытательный полигон самоходных транспортных средств, инструментальный полигон гуманитарной помощи в случае стихийных бедствий или инструментальная домашняя среда). Такие ресурсы помогут установить и поддерживать стандарты бенчмаркинга, позволяющие измерять прогресс исследований с помощью сопоставимых подходов и тестирования воспроизводимости.

Испытательные стенды должны поддерживать эксперименты как с новым программным, так и с аппаратным обеспечением, оснащённым богатыми возможностями для моделирования физического мира. Поддерживаемые моделируемыми, живыми и смешанными средами, эти платформы будут поддерживать исследования и эксперименты, которые разрешают открытые, реальные проблемы. Кроме того, они должны быть сконструированы таким образом, чтобы обеспечить сбор ценных данных, которые могли бы быть доступны сообществу для обучения и оценки, обеспечивая дополнительное топливо для прогресса.

Меры для Управления научно - технической политики:

• Координация инвестиций агентства в испытательные стенды для исследований и разработок в области искусственного интеллекта

Национальная инициатива по ИИ должна координировать инвестиции агентства в испытательные стенды ИИ в рамках ежегодного бюджетного

процесса, согласовывая инвестиции с приоритетами исследований, сформулированными в стратегическом плане инициативы. Следует сосредоточить внимание на модернизации существующих ресурсов для поддержки технологий, основанных на данных и ИИ.36

Действия для федеральных агентств:

• Инвестируйте в предметно-ориентированные испытательные стенды ИИ с помощью модернизированных или специально построенных объектов

Инвестиции в набор национальных испытательных стендов ИИ должны осуществляться несколькими федеральными агентствами, способствуя созданию предметно-ориентированных ресурсов, открытых для более широкого исследовательского сообщества. Основные направления деятельности каждого испытательного стенда должны быть согласованы с приоритетными направлениями исследований ИИ и поддержаны существующими федеральными инвестициями в ИИ.

Испытательные стенды должны быть созданы как «пользовательские объекты», которые поддерживают гибридный подход предоставления грантов для использования и взимания платы с тех, кто не был выбран для финансирования грантов. Плата за использование будет способствовать поддержанию испытательных стендов и дополнительного объема финансирования, выделяемого на гранты.

Действия для Конгресса:

• Поддержка запросов агентства о финансировании создания испытательных стендов для исследований и разработок в области искусственного интеллекта.

Компонент: Инвестирование в крупномасштабные открытые учебные данные

Данные являются важнейшей валютой для современных популярных подходов к ИИ. Перспективная работа в области низкоуровневого обучения, полууправляемого обучения и обучения на основе синтетических данных высвечивает будущее, в котором производительность системы ИИ не будет

напрямую связана с большими данными, и федеральное правительство должно продолжать уделять приоритетное внимание финансированию исследований в этих областях. Однако балансирование этих ставок на будущее дальнейшее развитие США с инвестициями в ресурсы для лидерства в современных ведущих подходах к ИИ укрепит фундамент как нынешних, так и будущих технологий и приложений на основе ИИ.

Создание систем ИИ и решений для новых областей и сфер применения зависит от наличия специализированных данных, которые были подготовлены и организованы для использования. Федеральная поддержка хорошо разработанных, общедоступных наборов данных и предоставление готовых к использованию ИИ правительственных наборов данных поможет стимулировать прогресс исследований в области ИИ и его применения в других областях исследований. В настоящее время значительный объём государственных данных, которыми можно легально делиться с доверенными негосударственными исследователями, не передается из-за отсутствия доверия к технологиям кибербезопасности и защиты частной жизни, а также из-за отсутствия готовности принимать риск.

Ответственное создание конвейеров для курации, размещения и обслуживания сложных наборов данных заложило бы основу для будущих возможностей ИИ, помогло бы стратегически направить исследовательское сообщество к вопросам, представляющим общественный интерес, и продвинуло бы технологии вокруг поддержания жизненного цикла наборов данных.

Эти инвестиции в данные могут быть дополнительно поддержаны созданием доменных тестовых площадок, рекомендованных выше, и размещены через NAIRR. Такая интеграция могла бы способствовать созданию наборов данных для поддержки контрольных показателей в рамках тестовых стендов, а также генерировать наполненные данные из тестирования, которые могли бы в свою очередь быть предоставлены для обслуживания исследовательского сообщества. Доступ к ресурсам должен предоставляться

исследователям, имеющим проверенные исследовательские достижения, и регулироваться соответствующими мерами контроля на соответствие оснований типу данных и метаданных, содержащихся в наборе данных.

Действия для Исполнительной власти:

• Разработать общую политику и выбрать лучшие практики.

Используя работу NIST,37 главный специалист по данным США должен разработать общую политику и выбрать лучшие практики для поддержки выпуска готовых к ИИ правительственных данных для общественности, а также работать с промышленностью и академическими кругами над принятием совместимой политики по лучшим практикам для документирования и взаимного обмена.

• Обеспечить стимулы для промышленности и научных кругов к предоставлению отдельных наборов данных.

Главный специалист по данным США должен разработать стимулы для промышленности и научных кругов, чтобы сделать доступными отдельные наборы данных по NAIRR, которые будут управляться и будут доступны наряду с государственными наборами данных.

• Поддержите исследователей кибербезопасности и конфиденциальности, финансируемых NSF, чтобы сделать правительственные данные доступными для исследовательских целей.

Национальная инициатива по ИИ должна координировать финансируемые NSF исследования в области кибербезопасности и конфиденциальности для выполнения ротационных заданий в федеральных агентствах38 и тесно сотрудничать с персоналом агентства и управляющими данными, чтобы ответственно разблокировать доступ к большему количеству государственных хранилищ данных с целью стимулирования исследований и инноваций в области ИИ.

Исследователи будут применять многообещающие методологии для защиты данных и конфиденциальности контролируемым образом, обеспечивая доказательную базу для новых подходов и объективных доказательств в целях

обоснования эволюционирующей политики и практики обмена данными. Это может включать в себя создание безопасной среды для проверенных исследователей для обеспечения их доступа к более чувствительным правительственным данным.

Действия для Конгресса:

• Разблокировать общедоступные данные для исследований и разработок в области искусственного интеллекта.

Конгресс должен финансировать команды инженеров и учёных по обработке данных, организованные через Цифровую службу США, чтобы разблокировать публичные данные, которые в настоящее время хранятся правительством для использования исследовательским сообществом ИИ.39

Эти команды будут расставлять приоритеты, подготавливать и курировать несекретные публичные наборы данных, чтобы сделать их готовыми к ИИ, структурировать устойчивые процессы для сбора, очистки и регулярного обновления данных, которые будут размещаться на платформе, такой как NAIRR, доступной проверенным американским исследователям.

• Финансировать программу обработки данных ИИ в Министерстве энергетики.

Конгресс должен выделять 25 миллионов долларов в год в течение следующих пяти лет для управления программой данных ИИ, которая будет создавать образцовые, сложные наборы данных и поддерживать их в качестве живых, регулярно обновляемых ресурсов. Они могут включать специализированные наборы данных по физическим, биологическим, земным и инженерным наукам, а также по социальным наукам.

Эта программа должна координироваться через Национальную инициативу по ИИ, чтобы обеспечить создание наборов данных, направляющих исследовательское сообщество в нужных направлениях.

Конгресс должен поручить DoE тесно сотрудничать с NIST в разработке стандартов для данных, включая стандарты для документации, моделирования данных, проектирования данных и форматов данных, а также для продвижения

методов и инструментов, необходимых для поддержки жизненного цикла данных.

Компонент: Спонсирование Открытой сети знаний

Открытые сети знаний (или хранилища) с огромными объёмами мировых знаний могут подпитывать следующую волну исследований ИИ, продвигая инновации от научных исследований к коммерческому сектору. Сегодня только крупнейшие технологические компании имеют ресурсы для разработки значительных графов знаний и сетей.

Различные федеральные агентства инвестировали средства в специализированные, предметно-ориентированные сети знаний, которые могли бы стать отправной точкой для создания открытой сети знаний. Начав со стремления объединить и сопоставить существующие специализированные сети знаний и правительственные платформы данных, а затем опираясь на реальные знания и контекст, правительство могло бы спонсировать Открытую сеть знаний, которая служила бы проверенным американским компаниям и исследователям всех слоев общества для использования мировых знаний при разработке систем искусственного интеллекта, работающих эффективно и действенно. Этот тип ресурсов, особенно в сочетании с дополнительной исследовательской инфраструктурой, описанной выше, может открыть границы еще не исследованных технологий.

Меры для Управления научно - технической политики:

• Провести инновационный спринт для создания дорожной карты открытой сети знаний.

Используя предыдущую работу,проделанную в рамках Межведомственной рабочей группы по сетевым исследованиям и разработкам в области информационных технологий (НИТРД),43 Управление научно-технической политики должно провести инновационный спринт для разработки дорожной карты поэтапного создания открытой сети знаний.

Действия для Конгресса:

• Непосредственное финансируемое внедрение и управление сетью открытых знаний.

Конгресс должен направлять и финансировать NSF для внедрения и управления сетью открытых знаний, выделяя 25 миллионов долларов в год в течение следующих пяти лет и поощрять NSF использовать партнерские отношения с заинтересованными сторонами тех отраслей, где это возможно.

Рекомендация

Рекомендация: Использовать обе стороны государственно-частного партнерства

Американские компании находятся на переднем крае AIR&D, и их инвестиции приносят пользу потребителям во всём мире благодаря быстрой разработке и внедрению продуктов с поддержкой искусственного интеллекта. Но влияние продуктов с поддержкой искусственного интеллекта на американское общество и национальную безопасность в значительной степени стало запоздалым. Скорость развития технологий частным сектором значительно опережает федеральную политику и нормативные акты. Чтобы решить эти проблемы, государственный и частный сектор должны разделить ответственность за безопасность и благополучие американцев. Следующие рекомендации сделают правительство лучшим партнёром для промышленности и расширят преимущества таких стратегических новых технологий, как ИИ, через региональные инновационные кластеры, а также расширят возможности доступа к исследованиям и образованию в области ИИ через благотворительность частного сектора.

Компонент: Создание рынков для ИИ и других стратегических технологий

Покупательная способность правительства не может конкурировать с глобальным потребительским рынком, но она может влиять на инвестиционные решения в технологиях, необходимых для общего технического лидерства США.45 Многие потенциальные приложения ИИ в государственном секторе, такие как образование и труд, подпадают под действие агентств с

ограниченными бюджетами на НИОКР. Поскольку правительство увеличивает инвестиции в фундаментальные исследования, оно также должно полностью использовать свою покупательную способность для поддержки ИИ и других стратегических технологий. Масштабы государственного финансирования могут влиять на приоритеты исследований и жизнеспособность стартапов на ранних стадиях, которые часто преуспевают или терпят неудачу уже в первый год, и если использовать их коллективно, они могут привлечь ресурсы частного сектора в области стратегического приоритета. Это сделает инвесторов и технологические компании важными партнерами для AIR&D, способствующими созданию будущего потенциала обороны и национальной безопасности.

Тем не менее правительство остается сложным заказчиком – особенно для малого и среднего бизнеса из-за сложного процесса заключения контрактов и уникальных требований. Превращение правительства США в более привлекательного клиента и эффективного покупателя коммерческих технологий поможет стимулировать развитие технологий в коммерческом секторе, отвечающем национальным интересам. Она также будет помогать правительству практически во всех аспектах его миссии – от предоставления основных государственных услуг до проведения экономической политики и защиты национальной безопасности.

Действия для Администрации общего обслуживания (GSA):

• Содействовать применению ИИ в правительстве США.

Обладая мандатом на содействию внедрению технологий ИИ в федеральном правительстве,47 Центр передового опыта ИИ (AI CoE) должен в первую очередь обратить внимание на легкодоступные готовые коммерческие технологии (COTS), которые могут быть адаптированы для использования правительством.

AI CoE ИИ необходимо работать с федеральным техническим руководством, включая Главного технического директора США, Советом Главного информационного директора и Национальной инициативы ИИ, чтобы

определить государственные потребности и возможности для ускорения принятие коммерческих приложений ИИ в федеральных агентствах.

AI CoE ИИ должен использовать существующие усилия по цифровому управлению в рамках Исполнительной власти, включая 18F GSA и Цифровую службу США, а также программы обмена техническими талантами с включением Президентской инновационной стипендии GSA, чтобы привнести в эти усилия достаточно технического опыта и коммерческой компетентности.

• Сообщать частному сектору о приоритетах федерального потенциала в области ИИ.

Aicpa должна увеличить приоритет федеральных закупок и потребностей агентства в потенциале на своём общедоступном веб-сайте, содержащем информацию о программах, пилотных проектах и других инициативах.

Действия Администрации малого бизнеса США:

• Опубликовать цифровую технологию «playbook» для малого бизнеса.

Учебник для малого бизнеса должен очертить пути для компаний, заинтересованных в ведении бизнеса с правительством США, и объяснить, как ориентироваться в таких проблемах, как, например, получение карты доступа в государственные учреждения. Такой ресурс сделал бы процесс приобретения более прозрачным и уменьшил бы потребность компаний в привлечении внешней помощи.

Книга должна быть разработана и рассмотрена персоналом с техническим и коммерческим опытом, например, Президентскими инновационными стипендиатами или сотрудниками Цифровой службы США, и написана на языке, который могут понять технологические стартапы, не имеющие опыта работы в правительстве.

Содержание книги следует активно рекламировать, чтобы повысить ее видимость для бизнеса.

• Объединение государственных и частных инвестиций в рамках Программы инновационных исследований малого бизнеса (SBIR).

Поддерживайте усилия федеральных агентств по модернизации SBIR для более эффективной разработки и внедрения решений ИИ; поощряйте более широкое участие американских технологических стартапов и компаний малого бизнеса.

Расширьте пилотные программы, которые предлагают дополнительное финансирование для преодоления разрыва между текущими премиями SBIR/Small Business Technology Transfer (STTR) Phase II awards и усилиями по масштабированию фазы III.

Расширьте пилотные программы, которые предлагают более крупные объемы финансирования и соответствующие возможности частного сектора для поддержки более высоких уровней технологической готовности, характерных для контрактов DoD SBIR.

Обновите Директиву политики SBIR, чтобы позволить программам соответствовать требованиям частного сектора уже на этапе II.

Действия для Министерства обороны и разведывательного сообщества:

• Принять модель «hoteling», позволяющую малым и средним технологическим компаниям получать доступ к секретным объектам на гибкой основе.

Цифровая экосистема, создаст прототипическую среду платформы для участников и пользователей, включая подготовленный персонал из компаний ИИ. Гибкий доступ к секретным помещениям ускорит циклы разработки и поможет компаниям более регулярно взаимодействовать с текущими или потенциальными клиентами в рамках предприятия национальной безопасности, что быстрее приведет к более индивидуальным и эффективным поставляемым решения.

• Упрощение процесса заключения контрактов для привлечения нетрадиционных поставщиков.

Внести поправки в Федеральное положение о закупках в сфере обороны, чтобы обеспечить более широкое рассмотрение коммерческих показателей в процессе заключения контрактов. Правительство США может извлечь выгоду

из более широкого внедрения лучшего в своем классе коммерческого программного обеспечения ИИ.

Разрешить пилотное использование коммерчески доступных цифровых прикладных инструментов и порталов доступа для SBIR и других нетрадиционных транспортных средств.

• Взять на себя обязательство по расширению инновационной базы национальной безопасности.

Минобороны должно поставить задачу увеличить число своих контрактов с технологическими фирмами на ранних стадиях в четыре раза в течение пятилетней Оборонной программы будущих лет.59 Это также потребует увеличения бюджетов зарождающихся, но успешных инновационных инициатив, таких как Подразделение оборонных инноваций.60

До этого момента Министерство обороны сосредоточилось на большом количестве мелких ставок, не прибегая к более крупным инвестициям на более поздних стадиях. Более крупные контракты для более поздних компаний помогут масштабировать проверенные решения, отвечающие военным требованиям.

Заместителю министра обороны по закупкам и поддержке и Руководителям Служб закупок следует поощрять программы закупок всех размеров, и запрашивать заявки по крайней мере от одного нетрадиционного подрядчика на каждую программу.

• Повышение рентабельности инвестиций SBIR.

Пересмотр, модернизация и рационализация процессов SBIR для поощрения более широкого участия американских технологических стартапов и компаний малого бизнеса.61

Сотрудники программы должны чётко сообщать об этапах перехода, включая их критерии и суммы в долларах лауреатам SBIR, чтобы они могли планировать и выделять соответствующие ресурсы.

Разрешить контрактам SBIR использовать любой «цвет денег» в качестве суммы финансирования соответствующих фондов, вплоть до финансирования SBIR.

Обеспечить масштабирование успешных прототипов за счет достаточного финансирования, раннего доступа к клиентам и операторам и лучшей должной осмотрительности в отношении перспектив коммерциализации компании.62

Программы SBIR Военной службы и Управления Министра обороны (OSD) должны выделять часть финансирования SBIR для масштабирования успешных проектов SBIR посредством улучшений фазы II.63

Программные офисы должны предоставлять программные доллары наряду с соответствующими фондами SBIR, чтобы повысить вероятность перехода.

Продолжение мероприятий по приведению программы SBIR в соответствие с технологическими приоритетами Департамента для сосредоточения инвестиций на множестве ключевых технологий, в которых частный сектор может помочь НИОКР продвинуться вперёд.64

Управление заместителя министра обороны по научным исследованиям и инженерным разработкам должно ввести специальный запрос на ИИ, который предлагает решения по различным подходам ИИ65 и целому ряду уровней технологической готовности.66

Компонент: Формирование Сети региональных инновационных кластеров, ориентированных на Стратегические новые технологии

Конкуренция имеет решающее значение для динамичной инновационной базы национальной безопасности.67 Если в стратегической отрасли отсутствует конкуренция, одна неверная ставка действующего президента может поставить под угрозу технологическое лидерство страны.68 Правительство США должно создать среду, в которой инновационные стартапы смогут разрушать неэффективные или устаревшие способы ведения бизнеса и сами превратиться в лидеров отрасли. Правильное сочетание политики и стимулов может помочь

фирмам преодолеть растущие барьеры для выхода на передний край новых технологий, таких как ИИ. Такой подход будет способствовать инновациям в отраслях, которые необходимы для лидерства США в области ИИ, а также экономической и технологической конкурентоспособности страны в более широком смысле.

Как отметила Комиссия в своем Промежуточном докладе за 2019 год, кластеризация технологических фирм в таких регионах, как Силиконовая долина, приводит к более динамичной и глобально конкурентоспособной отрасли, ускоряя обмен знаниями и обостряя внутреннее соперничество. Однако эта тенденция принесла пользу некоторым регионам и демографии больше, чем другим. Чтобы стимулировать региональные инновации в более широких масштабах страны, правительство США должно поддерживать рост технологических кластеров в регионах со скрытым инновационным потенциалом. Более широкая по своей миссии и масштабу, чем существующие модели в правиительстве США, такая инициатива демократизирует доступ к федеральным ресурсам НИОКР, чтобы малые фирмы могли конкурировать в таких отраслях с высокими барьерами для входа, как ИИ. Содействуя обмену технологиями и талантами между государственным и частным секторами, правительство США также будет иметь хорошие возможности для заключения новых контрактов и соглашений о разделе интеллектуальной собственности на коммерческие технологии, которые имеют решающее значение для национальной безопасности США.

Действия для Конгресса:

• Создать межведомственный программный офис, ответственный за координацию сети региональных инновационных кластеров, ориентированных на НИОКР и коммерциализацию стратегических новых технологий.

Программный офис должен быть размещен Министерством торговли в NIST и укомплектован представителями департаментов и агентств США, имеющими опыт работы и миссией, связанной со стратегическими новыми

технологиями. Бюро должно также опираться на опыт частного сектора и академических кругов в рамках программы обмена талантами и внешних консультативных механизмов.

Конгресс должен выделить 5 миллионов долларов на создание прграммного офиса и поручить ему определить региональные инновационные кластеры в квалифицированных местах по всей территории Соединенных Штатов на основе конкурсного процесса, как это подробно описано ниже. В качестве первого шага программный офис должен запросить заявки на финансовую помощь от заявителей, ориентированных на НИОКР и коммерциализацию стратегических новых технологий. При оценке заявок программный офис должен учитывать следующие критерии:

Местоположение. Кластеры должны быть равномерно распределены по всей территории Соединенных Штатов, в регионах со скрытым инновационным потенциалом, с учётом таких факторов, как близость к федеральным научно-исследовательским центрам, уровень поддержки со стороны государственных и местных органов власти, наличие ценных предложений для ведущих фирм и научно-исследовательских институтов, а также размер и уровень образования местной рабочей силы.

Предметная область. Кластеры должны быть организованы вокруг исследований, разработок и коммерциализации стратегических новых технологий, которые имеют решающее значение для национальной конкурентоспособности США. Особый интерес представляют технологии, которые позволяют развиваться в смежных секторах и внутреннее производство которых непосредственно принесет пользу национальной безопасности США, такие как микроэлектроника.

Экономическая целесообразность. Чтобы максимизировать воздействие федеральных ресурсов и обеспечить самоокупаемость кластеров, финансовая помощь должна предоставляться только тем заявителям, которые демонстрируют наличие зарождающегося кластера в своем регионе.

Программный офис должен создать Технологические исследовательские центры (ТРЦ) для каждого кластера, чтобы облегчить сотрудничество между участниками. Формируя устойчивые партнерские отношения с якорными институтами, каждый кластер должен стремиться продвигать исследования, разработки и коммерциализацию стратегических новых технологий.

Использовать талант. ТРЦ должны принимать исследователей по временным поручениям от департаментов и агентств США, организовывать обмен талантами с местными фирмами и исследовательскими институтами и финансировать многолетние постдокторские стипендии для коммерциализации исследований.

Поощрять передачу технологий. ТРЦ должны принимать руководителей программ из департаментов и агентств США, ответственных за перевод фундаментальных исследований в коммерчески жизнеспособных технологий, выявлять случаи использования национальной безопасности и конечных пользователей в правительстве США и инициировать новые государственные контракты на эти продукты.

Создание интеллектуальной собственности. ТРЦ должны заключать соглашения о разделе интеллектуальной собственности с участниками кластера, чтобы стимулировать принятие правительством коммерческих технологий. Когда это уместно, исследования должны публиковаться в открытом доступе, чтобы стимулировать прогресс в более широком научно-техническом сообществе.

Приведите в действие правительственные ресурсы. ТРЦ должны облегчать участникам доступ к федеральным вычислительным ресурсам, курируемым правительственным наборам данных, тестовой инфраструктуре и полигонам, а также другим объектам НИОКР при низких затратах.

Программный офис должен играть координирующую роль высокого уровня, которая включает в себя надзор за функционированием ТРЦ, содействие сотрудничеству в области НИОКР между кластерами и содействие

коммерциализации технологий с использованием примеров национальной безопасности.

• Принять пакет положений, стимулирующих промышленность и научные круги к участию в кластерах.

Резервы должны включать налоговые льготы для размещения вблизи кластера, конкурсные исследовательские гранты, кредитные гарантии и начальное финансирование. Органы государственной власти и местного самоуправления должны применять взаимодополняющий подход. Эта политика может быть смоделирована на основе зон применения, которые стимулируют инвестиции в региональную экономику.

Инвестиционные налоговые кредиты. Чтобы конкурировать со стимулами, предлагаемыми зарубежными странами, Конгресс должен установить инвестиционные налоговые льготы для фирм, участвующих в региональных инновационных кластерах. Хотя детали этих налоговых льгот будут варьироваться в зависимости от отрасли, одним из примеров является инвестиционный налоговый кредит для предприятий по производству полупроводников.

• Обеспечить финансирование каждого кластера не менее чем на пять лет с соответствующими инвестициями со стороны партнеров из государственного и частного секторов.

В течение одного года программный офис должен запросить у Конгресса финансирование, необходимое для 10 кластеров. Это финансирование должно быть сопоставимо, по крайней мере, 1:1 с инвестициями частных компаний, государственных и местных органов власти и федеральных агентств, причем цель каждого кластера изначально состоит в том, чтобы ежегодно получать в общей сложности 50 миллионов долларов. Эта ежегодная сумма должна увеличиваться по мере того, как будут расширяться со временем спрос и потенциал в каждом кластере. Эти средства будут использоваться для эксплуатации ТРК, обслуживания научно-исследовательских центров, выдачи исследовательских грантов и посевных стартапов.

Компонент: Создание конкурентоспособного Консорциума под руководством частного сектора

Частный сектор разделяет с правительством ответственность за укрепление основ экосистемы НИОКР, лежащей в основе прорывов, которые они будут коммерциализировать, и системы подготовки кадров, необходимой для удовлетворения растущего спроса на технические таланты.

Компании уже борются за то, чтобы найти этих квалифицированных кандидатов на технические должности, по оценочным данным, по всей стране более 400 000 открытых компьютерных рабочих мест.82 Кроме того, как описано выше, исследователи в академических кругах, проводящие исследования с высоким риском и высокой прибылью, оказываются отрезаны от вычислительных и информационных ресурсов, необходимых для подпитки этой работы. То, насколько хорошо страна справляется с этой надвигающейся проблемой, имеет широкие последствия для экономики, общества и глобальной конкурентоспособности США.

В главе 10 этого доклада подробно описываются рекомендации по модернизации системы образования США для подготовки американцев к работе в будущем, и подробно описываются обширные инвестиции федерального правительства в исследования и разработки в области ИИ. Однако корпорации должны также учитывать свою ответственность за подготовку граждан к будущему, которое они изобретают, и поддерживать прочный фундамент национальных инноваций, от которых они получают прибыль. С этой целью многие фирмы уже оказывают положительное влияние за пределами своих конечных результатов благодаря усилиям по обеспечению корпоративной социальной ответственности. Программы STEM-образования и профессиональной подготовки занимают видное место в благотворительной деятельности ведущих технологических фирм.83 Однако масштабы проблемы слишком велики, чтобы отдельные фирмы могли решить ее в условиях инсоляции, несмотря на свою щедрость.

Меры в интересах частного сектора:

• Пожертвовать 1 миллиард долларов в течение пяти лет

Предоставление каждому американцу возможности повысить свой технический уровень требует смелых действий со стороны правительства, научных кругов и промышленности по координации, приоритизации и масштабированию программ, расширяющих возможности исследований ИИ и прививающих цифровые навыки. Для того чтобы частный сектор выполнил этот призыв к действию, Комиссия призывает промышленность пожертвовать 1 миллиард долларов в течение следующих пяти лет на поддержку образования и повышения квалификации в области искусственного интеллекта, а также предоставить данные и вычислительные ресурсы в целях демократизации и поддержки лучших в своем классе исследований в области ИИ.

Эти средства заложат основу для более широкой цифровой трансформации и расширения экономических возможностей. Государственные чиновники должны публично освещать влияние этих мероприятий и роль фирм, вносящих в них свой вклад.

Подобно Партнерству по работе ИИ, координирующему разработку лучших практик между фирмами ИИ, эти мероприятия должны управляться независимой некоммерческой организацией, которая может связать и масштабировать усилия фирм по созданию цифровых навыков и демократизации исследований ИИ. Академия цифровых услуг США, предложенная Комиссией, могла бы также предоставить экспертные знания, добровольцев, разработку учебных программ и другую поддержку.

• Расширить научно-исследовательские обмены между промышленностью и академическими кругами.

Ведущие технологические компании должны инвестировать или расширять программы обмена, предназначенные для объединения лучших академических талантов с компьютерными ресурсами частного сектора мирового класса. Ротационные обмены такого типа одновременно демократизировали бы доступ к вычислительной технике для исследователей и

одновременно пролили бы свет на пути создания продуктов ИИ следующего поколения, которые могли бы быть коммерциализированы промышленностью.

Действия Бюро статистики труда США:

• Стандартизировать и сообщать данные о цифровых навыках на рынке труда.

Бюро статистики труда США должно возглавить мероприятия в координации с другими ведомствами, например, Министерством образования, по сбору и регулярному обновлению статистических данных о цифровом мастерстве демографических групп и регионов с описанием конкретных цифровых навыков, необходимых фирмам, открывающим вакансии. Это позволит академическим учреждениям, фирмам и другим организациям расставить приоритеты в своих усилиях по обучению, переобучению, повышению квалификации и цифровой трансформации.

Рекомендация: Решите некоторые из самых больших проблем человечества

Если инвестиции, описанные выше, будут реализованы, они создадут условия для использования ИИ для решения некоторых из самых больших проблем в науке, обществе и национальной безопасности.

Примеры многообещающих инициатив, которые могли бы улучшить благосостояние общества и продвинуть научные рубежи, но не ограничиваются ими:

• Обеспечение долгосрочного качества жизни. Технология искусственного интеллекта может помочь пожилым людям жить самостоятельно дольше, помогая в управлении здоровьем и повседневными задачами, и улучшая качество жизни. Это может включать применение ИИ в биомедицине для решения острых и хронических заболеваний и улучшения здорового старения.

• Революционизировать образование и обучение на протяжении всей жизни. Инструменты ИИ, которые персонализируют образование, обучение и переподготовку на соответствующих уровнях сложности и интуитивно

оценивают развитие для оптимизации стандартных учебных программ, способствующих индивидуальному успеху в обучении.

• Трансформация управления энергией. Интеллектуальная инфраструктура для городов, способная эффективно реагировать на резкие скачки спроса на энергию и чрезвычайные ситуации (как техногенные, так и стихийные бедствия).

• Эффективное прогнозирование, моделирование, подготовка к стихийным бедствиям и реагирование на них. Точное, близкое к реальному времени обнаружение землетрясений и пожаров, прогнозирование эскалации для помощи в реагировании на чрезвычайные ситуации и планирования оптимального развертывания ограниченных ресурсов. Автономные роботы для поиска, спасения и очистки после природных или техногенных катастроф, оказывающие многократно увеличенную поддержку спасателям и специалистам по опасным материалам.

• Направить Национальную инициативу по ИИ на согласование федеральных инвестиций в НИОКР для решения значительных научных, технологических и социальных проблем.

Национальная инициатива по ИИ должна выявлять и контролировать реализацию возможностей использования федеральных инвестиций в НИОКР для решения смелых научно-технических задач, которые могут привести к прорывам на благо общества и национальной безопасности.

Приоритетность этих усилий должна координироваться с исследовательским сообществом национальной безопасности и определяться Советом по конкурентоспособности технологий, предложенным Комиссией, для выявления областей исследований, в которых применение ИИ могло бы способствовать прогрессу, обеспечивающему стратегические преимущества.

Интеллектуальная собственность

План действий

Американские законы и институты в области интеллектуальной собственности (ИС) должны рассматриваться как важнейшие компоненты защиты интересов национальной безопасности США, включая содействие экономическому процветанию и технологической конкурентоспособности. Приоритетность политики в области ИС особенно важна с учетом того, что Китай использует политику в области ИС в качестве инструмента для своих национальных стратегий по развитию новых технологий. Соединенные Штаты должны, как минимум, сформулировать и разработать национальные реформы и политику в области ИС с целью стимулирования, расширения и защиты искусственного интеллекта (ИИ) и новых технологий как внутри страны, так и за рубежом. Такая политика должна разрабатываться и предлагаться через Исполнительную власть с помощью процесса, объединяющего разрозненные департаменты и агентства, которые играют важную роль в продвижении инноваций в США.

Рекомендация: Разработать и внедрить национальную политику и режимы ИС для стимулирования, расширения и защиты ИИ и новых технологий в рамках стратегий национальной безопасности.

Действия для президента:

• Издать Исполнительный указ о приоритизации политики ИС в отношении ИИ и критических новых технологий.

Президент должен издать Исполнительный указ о признании политики в области ИС в качестве национального приоритета и установить всеобъемлющий процесс реформирования и установления новых политик и режимов в области ИС для ИИ и критических новых технологий, способствующих реализации стратегий национальной безопасности, экономики и технологической конкурентоспособности.

Исполнительный приказ должен:

Поручить вице-президенту в качестве Председателя Совета по технологической конкурентоспособности (ТСС) или иным образом в качестве

председателя межведомственной целевой группы осуществлять надзор за всеобъемлющим процессом;

Поручить министру торговли:

Руководить на постоянной основе разработкой предложений (действий исполнительной и/или законодательной ветвей власти) по реформированию и созданию новых политик и режимов ИС для стимулирования, расширения и защиты ИИ и новых технологий;

При выполнении этих обязанностей координируйте свои действия с заместителем Министра торговли по интеллектуальной собственности, директором Управления по патентам и товарным знакам США (USPTO) и другими соответствующими органами исполнительной власти; консультируйтесь с директором Управления по авторским правам США; и созывайте общественные обсуждения, включающие, как минимум, научные круги и промышленность;

Поручить директору ВПТЗ США в его качестве советника Президента4:

Представить в течение 90 дней вице-президенту в качестве главы ТКК или межведомственной целевой группы доклад, в котором (1) определяются и анализируются показатели, тенденции и данные, необходимые для информирования о разработке политики в области ИС, особенно в соответствии с приоритетами, указанными в Исполнительном указе; и (2) определяются соответствующие департаменты и агентства Исполнительной власти США, которые должны будут предоставить любые необходимые данные;

Представить в течение 12 месяцев с момента выпуска первого доклада вице-президенту второй доклад или отдельные его части на скользящей основе, которые (1) всесторонне оценивают слабые стороны нынешней политики и режимов ИС США по сравнению с режимами ИС других стран для стимулирования, расширения и защиты инноваций в области ИИ и новых технологий и поддержки национальных стратегий; (2) изучают неисчерпывающий перечень «соображений ИС» (см.); и (3) предлагает

соответствующие исполнительные и законодательные меры по реформированию и установлению новых политик и режимов в области ИС;

Предоставить вице-президенту всю необходимую информацию и консультации, чтобы обеспечить полный анализ предложений ИС;

Поручите вице-президенту:

Руководить текущей оценкой политики, режимов и предложений Министра торговли в области ИС, которые должны быть реализованы и интегрированы в стратегии национальной безопасности, экономической и технологической конкурентоспособности;

Наделить Министра торговли полномочиями содействовать осуществлению политики и режимов в области ИС, которые оцениваются как имеющие решающее значение для национальной безопасности, экономической и технологической конкурентоспособности; и

Поручить департаментам и учреждениям исполнительной власти обеспечить ресурсы и поддержку Министра торговли в выполнении этих усилий по исполнению Указа, включая предоставление выявленных показателей и тенденций.

Действия для министра торговли и директора ВПТЗ США:

• Создать по мере необходимости, в рамках консультации с директором ВПТЗ США, комитет междисциплинарных экспертов как внутри правительства США, так и за его пределами для предоставления технических и связанных с ИС экспертных знаний и консультаций при осуществлении настоящего Исполнительного Указа.

• Провести публичные обсуждения, включив, как минимум, академические и промышленные круги в выполнение этих обязанностей по исполнению Указа. Результаты этих обсуждений должны стать основой для предлагаемой политики и режимов ИС.

• Оценка показателей и данных, необходимых для обоснования политики в области ИС.

При оценке надлежащих показателей и данных, необходимых для обоснования обсуждения политики в области ИС, как того требует Исполнительный указ, Министр торговли и директор ВПТЗ США должны использовать общегосударственный подход. Из-за широты соображений ИС, в том числе изложенных в настоящем докладе, а также далеко идущего влияния ИС на многие сегменты экономики и инновационной экосистемы США, существует множество государственных структур, которые уже могут отслеживать соответствующие показатели или иметь возможность расширить свой анализ для решения вопроса о необходимой приоритизации ИС для ИИ и новых технологий.

Например, тенденции в области инноваций и инвестиций, основанные на патентных заявках, и, по возможности, данные о лицензировании в различных технологических секторах, в том числе в зарубежных странах, особенно в Китае, должны анализироваться (например, для оценки качества и тенденций в области исследований5) с осторожностью, чтобы не полагаться исключительно на подсчёт патентов.

Другие потенциальные показатели включают, но не ограничиваются, отслеживанием патентов, объявленных стандартами более существенными по сравнению с патентами, фактически лицензированными; лицензирование несвязанных сторон; влияние предшествующего уровня техники на систему экспертизы патентов и товарных знаков США; международные заявки на защиту ИС на финансируемые США исследования, особенно без ведома американских спонсоров или изобретателей; соотношение американских компаний, подающих заявки на защиту ИС, а также ведущих судебные процессы, связанные с ИС, в США и за рубежом; данные о присвоении патентов.

Меры для Министерства юстиции:

• Консультировать суды по вопросам обеспечения последовательности решений о патентоспособности;

Министерство юстиции через Генерального солиситора и Гражданскую апелляционную секцию должно консультировать федеральные суды по устранению запутанных, непоследовательных или чрезмерно ограничительных решений о патентоспособности для обеспечения соответствия политике национальной безопасности.

Действия для Конгресса:

• Приоритетность предлагаемого законодательства в области ИС для укрепления национальных стратегий США, в том числе в области национальной безопасности, экономических интересов и технологической конкурентоспособности.

Конгресс должен уделять приоритетное внимание законодательным рекомендациям по политике и режимам ИС, выдвинутым вице-президентом в качестве председателя ТКК или межведомственной целевой группы. Это особенно важно с учётом того, что Конгресс несёт ответственность за принятие законодательства о патентах и ИС, которое ВПТЗ США и другие соответствующие заинтересованные стороны выполняют и соблюдают. Кроме того, Управление авторского права США размещено в качестве федерального департамента в Библиотеке Конгресса в качестве главного советника Конгресса по вопросам авторского права и управляет регистрацией авторских прав.6

Исполнительный указ о приоритизации политики в области ИС для ИИ и новых технологий*

*Эта иллюстрация не является исчерпывающей для всех соответствующих государственных структур США, несущих ответственность за интеллектуальную собственность.

Рекомендация: Министру торговли следует оценить и изучить следующий неисчерпывающий перечень «соображений ИС» в координации с заместителем Министра торговли по ИС и директором ВПТЗ США в рамках разработки и предложения вице-президенту реформ и новых стратегий и режимов в области ИС.

Меры для министра торговли:

• Оценить и изучить нижеследующий неисчерпывающий перечень из 10 соображений, касающихся интеллектуальной собственности, в рамках докладов, представляемых вице-президенту в соответствии с Указом Президента.

1. Патентное право: Министр торговли должен оценить и сформулировать влияние действующих законов о патентном праве на инновации в области искусственного интеллекта и новых технологий с точки зрения экономической, торговой политики и политики национальной безопасности, чтобы лучше информировать законодательные и ведомственные усилия по реформе патентного права. Американский режим интеллектуальной собственности стимулировал американскую изобретательность с конца 18-го века. Защищая «любой новый и полезный процесс, машину, производство или состав вещества» с помощью стабильных правовых институтов, управляемых верховенством закона, изобретатели и инвесторы полагались на американскую систему ИС, чтобы обеспечить определенность, необходимую для оправдания крупных и рискованных инвестиций в НИОКР,7 которые имеют решающее значение для технологий.8 Сильная и надежная патентная система в равной степени важна для стимулирования американских инноваций в области ИИ и новых технологий, влияющих на национальную безопасность. К сожалению, недавние судебные решения по патентному праву сузили круг изобретений, подлежащих патентной охране. Это привело к широкому спектру инноваций, которые в настоящее время не подлежат патентной защите как в области цифровых технологий, так и в области биофармы. Правовая неопределенность в США для компаний новаторов в отношении того, будут ли их изобретения иметь право на патентную защиту или могут быть признаны недействительными после получения патента, широко распространены. Эта неопределенность, в свою очередь, повлияла на инвестиции в ИИ и технологии, критически важные для национальной безопасности. Эмпирические исследования доказали, что патенты причинно связаны с венчурными инвестициями в стартапы и, как следствие, связаны с успехом стартапов.

Однако недавние отчеты показывают, что инвестиции в патентоемкие американские стартапы, разрабатывающие критические технологии (например, компьютерное оборудование, полупроводники, медицинские приборы и материалы, фармацевтические препараты и биотехнологии), сократились по сравнению с непатентоемкими компаниями. Это согласуется с тем, что инвесторы постоянно сообщают о том, что патентное право является ключевым фактором при принятии ими решений об инвестировании в технологии конкретной компании или выводе нового продукта на рынок.

Законодательство, по-видимому, является единственным практическим средством реформирования доктрины патентного права. Судебные органы, в частности Верховный суд, указали на нежелание пересматривать свои решения за последнее десятилетие, которые создали эту фундаментальную проблему в доктрине патентного права. ВПТЗ США приняло систему оценки патентного права в процессе экспертизы патентных заявок, которая дала положительные результаты в обеспечении большей определенности для заявителей на патент, но Федеральный округ, по-видимому, не склонен следовать рекомендациям ВПТЗ США.

Усилия по реформированию доктрины патентного права путем внесения поправок в соответствующее положение патентного законодательства потерпели неудачу в 2019 году.18 Точка зрения национальной безопасности не была выражена относительно влияния закона о патентном праве на технологии, имеющие решающее значение для национальной безопасности, такие как искусственный интеллект, микроэлектроника, телекоммуникации 5G, квантовые вычисления и биотехнологии. В основу национальной стратегии ИС должна быть положена точка зрения национальной безопасности на влияние действующих законов о патентном праве на ИИ и новые технологии.

2. Противодействие китайскому нарративу о победе в инновационном конкурсе: Министр торговли в координации с соответствующими департаментами и ведомствами (например, Государственным департаментом, USTR) должен рассмотреть вопрос о том, как Соединенные Штаты могли бы

наилучшим образом противостоять усилиям Китая по формированию представления о том, что он выигрывает инновационную конкуренцию, частично основанную на подаче патентных заявок и других вмешательствах на своих технологических рынках.19 Китай стал отечественным форумом с наибольшим количеством поданных патентных заявок, а китайские компании и изобретатели являются самыми плодовитыми подателями патентных заявок на ИИ во всем мире.20 Этот ориентир помогает сформировать представление о том, что Китай стал лидером в области инноваций, поскольку интенсивное патентование, как было показано, в целом коррелирует с экономическим ростом. Китай также завоевывает эту репутацию, когда речь заходит о новых технологиях, таких как ИИ. Источники утверждают, что Китай опережает Соединенные Штаты в подаче мировых патентных заявок, связанных с ИИ. Однако высокий уровень патентной продукции не обязательно свидетельствует о высоком уровне изобретательской продукции. В частности, нерыночные факторы, обусловленные вмешательством государства, могут искажать заявки. Кроме того, Китай часто подает патенты в качестве «игры чисел», что может привести к неправильной характеристике его технологического мастерства. Точно так же китайские компании 5G объявляют большинство патентов «существенными», по-видимому сочетая согласованную стратегию Китая сверху вниз по продвижению своей повестки дня в области искусственного интеллекта и новых технологий, влияя на установление международных стандартов с целью доминирования над числовыми ориентирами. Министру торговли следует рассмотреть вопрос о том, какие меры необходимо принять для того, чтобы уравновесить технологическое доминирование Китая, основанное на выборочных данных о патентовании.

3. Влияние подачи патентных заявок Китаем на ВПТЗ США и изобретателей США: Министр торговли в координации с директором ВПТЗ США должен оценить, требует ли ВПТЗ США дополнительных ресурсов, как людских, так и технических, для обеспечения качественной патентной экспертизы, и рекомендовать политику для решения любых проблем. При этом

Министр торговли должен оценить последствия увеличения числа заявок из Китая и предшествующего уровня техники, генерируемого искусственным интеллектом (термин в патентном праве для обозначения мировых научно-технических знаний, с помощью которых оценивается изобретение, чтобы определить, является ли оно новым). Большое количество часто некачественного уровня техники, созданного в результате крупномасштабного патентования Китая, потенциально может негативно повлиять на глобальные системы патентной экспертизы, включая системы ВПТЗ США.В то же время американские изобретатели могут столкнуться с препятствиями в патентовании огромного количества низкокачественного китайского предшествующего уровня техники. ВПТЗ США также отметило, что заинтересованные стороны подняли вопрос о том, может ли ИИ порождать распространение предшествующего уровня техники, что затрудняет поиск соответствующего предшествующего уровня техники для изучения.

4. Препятствия для государственно-частного партнерства и международного сотрудничества в области ИИ: Министр торговли должен оценить любые препятствия для контрактной экосистемы ИС в целях укрепления партнерских отношений ИИ между департаментами и агентствами национальной безопасности, промышленностью и международным сотрудничеством. Это должно включать оценку и устранение двусмысленностей в Федеральном регламенте закупок и Дополнении к Федеральному регламенту закупок обороны, имеющих отношение к ИИ и данным. Разработка ИИ представляет собой уникальные контрактные вопросы ИС. Например, отраслевым разработчикам ИИ, скорее всего, потребуется доступ к соответствующим правительственным учебным данным США для разработки правительственных решений или приложений с поддержкой ИИ. Если решение или приложение двойного назначения, частное лицо может захотеть предоставить лицензию правительственному агентству США на доступ к приложению ИИ, но сохранить IP-адрес в модели ИИ для лицензирования другим. Но остаются без ответа вопросы о том, имеет ли

правительственное агентство США какие-либо права ИС или права собственности на модель, которая была обучена на его данных. Правительство США может также захотеть сохранить права ИС, чтобы избежать «блокировки поставщиков». Эти нерешённые вопросы о правах ИС и вопросах собственности могут также возникнуть в международном сотрудничестве в области НИОКР в области систем искусственного интеллекта, где препятствия могут быть усилены противоречащими национальными законами об ИС и/или защите данных.

5. IP-защита данных: Министр торговли должен оценить, существует ли необходимость в защите sui generis или дополнительной защите данных типа IP, и предложить политику и/или законодательство, если защита будет сочтена необходимой. Данные имеют решающее значение для ИИ и машинного обучения (мл), но могут существовать пробелы в существующих режимах защиты, предоставляемых патентом или авторским правом. Неадекватная защита данных может лишить стимулов необходимые инвестиции в разработку этих критически важных наборов данных, а также соглашения о публичном раскрытии и совместном использовании. В то время как защита данных может стать будущей потребностью, США должны быть активными в оценке и решении необходимости такой защиты. Министр торговли также должен изучить способы защиты и стимулирования создания наборов данных, позволяя в какой-то момент обмениваться этими данными, особенно с более мелкими организациями, которые в противном случае не смогли бы выйти на рынок. В основу этой оценки должен быть положен анализ сильных и слабых сторон европейской системы защиты баз данных sui generis.

Борьба с кражей ИС: Министр торговли в координации с соответствующими департаментами и ведомствами (например, USTR, Координатор по защите интеллектуальной собственности, Национальный научный фонд, Управление научно-технической политики, а также Департаменты внутренней безопасности, юстиции, и государства) должен оценить и определить дополнительные усилия, которые Исполнительная власть

должна предпринять для противодействия угрозам кражи ИС, включая действия в сотрудничестве с союзниками и партнерами. В частности, министр торговли должен четко сформулировать, что США противодействуют – Стратегия хищения ИС будет содержать как криминальные, так и гражданско-экономические аспекты. Министерство торговли должно использовать все доступные инструменты для установления режима сдерживания, чтобы наказать фирмы, виновные в краже ИС США, и предотвратить будущие кражи ИС, чтобы выровнять игровое поле для американских и союзных фирм. Эти инструменты должны состоять во включении компаний-нарушителей в список организаций Бюро промышленности и безопасности, блокировании виз ключевым сотрудникам или взимания тарифов на продукты, полученные из украденных ИС. Решения, которые следует изучить, включают подготовку союзников и партнеров по пресечению контрафакции на границах и усилия по повышению уважения отдельных лиц к ИС и признанию контрафакции, а также способы ее предотвращения. Кроме того, Госсекретарю следует оценить методы и средства укрепления и обновления существующих механизмов, имеющихся в распоряжении американских жертв кражи коммерческой тайны, включая повторное введение законодательства об укреплении Закона об экономическом шпионаже путем, например, увеличения ущерба, доступного жертвам кражи коммерческой тайны, и продления срока давности.

7. Изобретательство ИИ: Министр торговли должен оценить необходимость изменения политики в отношении вопросов, возникающих в связи с изобретениями и творениями, созданными ИИ, особенно по мере развития технологий. ВПТЗ США определило, что в соответствии с действующей правовой доктриной изобретатель должен быть физическим лицом, и отказало в патентной заявке, в которой изобретателем была названа машина. США не одиноки в этом положении. ВПТЗ США также направило обширные запросы на публичные комментарии по целому ряду вопросов политики ИИ в области ИС, включая влияние ИИ на изобретательство и право собственности, а также воздействие на непатентную защиту ИС, такую как

авторское право. В результате ВПТЗ США опубликовало всеобъемлющий доклад с изложением мнений общественности о политике в области ИИ и ИС. Большинство комментаторов согласились с тем, что поскольку нынешние возможности ИИ ограничены «узким ИИ» (системами ИИ, которые обучаются и выполняют индивидуальные задачи в четко определенных областях), а искусственный общий интеллект еще не является реальностью, нынешний ИИ не может ни изобретать, ни создавать без вмешательства человека. Министру торговли следует проконсультироваться с союзниками и партнерами для обеспечения дальнейшей гармонизации различных вопросов ИС, возникающих в связи с изобретениями и творениями, созданными искусственным интеллектом, и получить представление о стратегиях Китая по решению этих проблем., особенно по мере того, как технологии ИИ выходят за рамки узкого ИИ.

8. Глобальное выравнивание IP-адресов: Министр торговли в координации с соответствующими департаментами и ведомствами (например, ВПТЗ США, ИПЕК, USTR, Министерство обороны, Государственный департамент) должен работать с партнёрами и союзниками над разработкой глобальных мер противодействия хищению интеллектуальной собственности и устранением любых несоответствий в патентных режимах, которые чрезмерно затрудняют компаниям защиту своих патентов на многонациональных рынках. При этом Секретари должны использовать рекомендацию Комиссии о том, чтобы Соединенные Штаты и союзники – через Формирующуюся технологическую коалицию – изучили скоординированные подходы к ИС (в рамках предложенной NSCAI критической области № 4: Поощрение и защита инноваций), включая взаимную повестку дня в рамках Дискуссии ВОИС по ИИ и ИС и форумов с более широкими мандатами. Секретари также должны оценить, являются ли существующие форумы для диалога по глобальному согласованию ИС достаточными или необходимы ли новые форумы или площадки, особенно с учётом любых изменений во внутренней политике или режимах ИС, выявленных в ходе рассмотрения других соображений ИС.

Например, если США определят, что необходимы новые меры политики защиты в отношении данных, им, возможно, придется работать с ключевыми союзниками и партнерами на двусторонней и многосторонней основе для обеспечения глобальной гармонизации.

9. Демократизировать экосистемы инноваций и ИС: Министру торговли следует оценить, необходимы ли дополнительные усилия исполнительной власти для расширения инновационной базы и демократизации доступа к экосистеме инноваций и ИС и создания большего числа рабочих мест. ВПТЗ США в сотрудничестве с Министром торговли предприняло инициативы по расширению инновационной базы США путём создания Национального совета по расширению американских инноваций (NCEAI) для разработки всеобъемлющей национальной стратегии повышения справедливости и стимулирования экономики США. Это инновационная экосистема путем поощрения, расширения прав и возможностей и поддержки всех будущих новаторов.46 Министр торговли должен обеспечить, чтобы ВПТЗ США пользовалось полной поддержкой Исполнительной власти в этих инициативах. В рамках инициативы NCEAI Министр торговли также должен сосредоточиться на оценке и выявлении потенциальных действий и инструментов, которые могут ускорить процессы и упростить руководство для стартапов, ищущих защиты ИС, а также обеспечить ресурсы для оказания помощи малым и средним предприятиям. Такое внимание особенно важно при сравнении влияния судебных издержек и потенциально чрезмерно обременительных процессов в США по сравнению с другими странами на решения американских изобретателей о защите ИС в Соединенных Штатах. 10. «Стандартный основной» патентный процесс: Министр торговли в координации с соответствующими департаментами и ведомствами (например, ВПТЗ США, NIST и Госдепартаментом) должен оценить политику, с помощью которой США могут играть ведущую роль и обеспечивать их безопасность. Фирмы могут в полной мере участвовать в процессах, посредством которых заявляются и утверждаются «стандартные существенные» патенты. Это

помогло бы обеспечить постоянную легитимность процесса установления стандартов частного метода, эффективную координацию разработки и внедрения новых технологий на рынке, а также предотвратить попытки Пекина доминировать или манипулировать этими процессами посредством собственной координации деятельности фирм из Китая. Руководство Коммунистической партии Китая чётко сформулировало связь между патентным лидерством в новых технологиях, таких как искусственный интеллект, и процессами установления стандартов для этих же технологий. Нынешние тенденции подтверждают намерение Китая использовать как патенты, так и стандарты для лидерства в технологических инновациях. Могут потребоваться дополнительные механизмы для защиты целостности международных стандартов, а также для защиты и поощрения инноваций США, такие как выявление усилий иностранных правительств по прямому или косвенному влиянию на организации, устанавливающие стандарты. Это также включало бы определение иностранных правительств, субсидирующих или иным образом стимулирующих чрезмерное декларирование патентов в качестве «основных стандартов» или создающих барьеры для участия США в иностранных органах по установлению стандартов. Министр торговли также должен изучить вопрос о том, каким образом правительство США могло бы поддержать небольшие американские компании и изобретателей, в полной мере участвующих в процессе установления стандартов, и поощрять наблюдение за лицензированием или юридическими спорами в иностранных юрисдикциях должностными лицами американских посольств и миссий. В связи с этим Министр торговли в координации с директором ВПТЗ США должен оценить решения иностранных судов о лицензировании, которые могут повлиять на национальный суверенитет США, чтобы определить согласованную позицию или ответ США.

Полученные данные.

Соединенные Штаты в значительной степени зависят от импорта некоторых микроэлектроник, жизненно важных для национальной

безопасности и экономического процветания. Эта зависимость от импорта полупроводников создает стратегическую экономическую и военную уязвимость для сбоев в цепочке поставок электроники, включая неблагоприятные действия иностранных правительств и стихийные бедствия. Несмотря на огромный опыт в области исследований, разработок и инноваций в области микроэлектроники по всей стране, Соединенные Штаты ограничены отсутствием отечественных предприятий по производству полупроводников, особенно для современных полупроводников. Это ограничение усугубляет риск того, что Соединенные Штаты могут опередить США в разработке и производстве микроэлектроники. Сосредоточение усилий правительства США, промышленности и научных кругов на развитии отечественных предприятий по производству микроэлектроники позволит снизить зависимость страны от импорта, сохранить США. лидерство в технологических инновациях, поддержка создания рабочих мест, укрепление национальной безопасности и торгового баланса, а также повышение технологического превосходства и боеготовности Вооруженных Сил, являющихся важными потребителями передовой микроэлектроники.

Политика. Для поддержания национальной безопасности и экономического процветания политика Соединенных Штатов должна быть направлена на то, чтобы опережать потенциальных противников в области современной микроэлектроники по крайней мере на два поколения и поддерживать многочисленные источники производства современной микроэлектроники в Соединенных Штатах.

Создание Подкомитета по руководству микроэлектроникой.

(a) Настоящим в Национальном научно-техническом совете учреждается подкомитет по вопросам лидерства и конкурентоспособности Соединенных Штатов в области микроэлектронных технологий и инноваций, который будет называться Подкомитетом по лидерству в области микроэлектроники (Подкомитет).

(b) Подкомитет состоит из следующих членов:

Министр торговли, который является председателем Подкомитета;

Государственный секретарь;

Министр обороны;

Министр энергетики;

Министр внутренней безопасности;

Директор Управления по вопросам управления и бюджета;

Торговый представитель Соединенных Штатов;

Директор национальной разведки;

Директор Национального научного фонда;

Помощник Президента по науке и технике;

Помощник Президента по вопросам технологической конкурентоспособности;

Помощник Президента по вопросам национальной безопасности;

Помощник Президента по экономической политике;

Помощник Президента по внутренней политике; и

Руководители других исполнительных департаментов и учреждений и другие старшие должностные лица в составе Исполнительной канцелярии Президента, как это определено Председателем.

(c) Закат. Подкомитет прекращает свою деятельность 1 января 2031 года.

Раздел 4. Функции Подкомитета по руководству микроэлектроникой. В соответствии с применимым законодательством Подкомитет:

(a) консультировать Президента по вопросам, связанным с политикой , затрагивающей микроэлектронику;

(b) разработать в течение 270 дней с даты настоящего приказа и не реже одного раза в пять лет после этого Национальную стратегию в области исследований, разработок, производства и безопасности цепочек поставок микроэлектроники (Стратегию), которая должна охватывать следующие элементы:

методы ускорения отечественной разработки и производства микроэлектроники и укрепления отечественной рабочей силы в области микроэлектроники;

методы обеспечения того, чтобы Соединенные Штаты были мировым лидером в области исследований и разработок в области микроэлектроники;

мероприятия, которые могут быть проведены для укрепления взаимодействия и информационно-пропагандистской работы между федеральными агентствами и промышленностью, научными кругами и международными партнерами Соединенных Штатов по вопросам, касающимся микроэлектроники;

приоритеты в области научных исследований и разработок в целях ускорения развития и внедрения инновационной микроэлектроники и новых видов применения микроэлектроники и компонентов;

роль дипломатии и торговли в поддержании позиций США как мирового лидера в области микроэлектроники;

потенциальная роль Федеральной лаборатории, центра или инкубатора, сосредоточенных исключительно на исследованиях и разработках микроэлектроники, как описано в разделе 231(b)(15) NDAA на 2017 финансовый год (как добавлено в разделе 276 NDAA на 2021 финансовый год) в реализации Стратегии; и

такие другие виды деятельности, которые, по мнению Подкомитета, могут оказаться целесообразными для преодоления будущих вызовов инновациям, конкурентоспособности и целостности цепочки поставок Соединенных Штатов в области микроэлектроники; и

(c) координировать процесс разработки политики в отношении связанных с микроэлектроникой исследований, разработок, производства и обеспечения безопасности цепочек поставок, а также бюджетов федеральных ведомств и обеспечивать соответствие такой деятельности Стратегии, предусмотренной настоящим разделом.

Общие положения.

(a) Если какое-либо положение настоящего приказа или применение такого положения будет признано недействительным, остальная часть настоящего приказа и другие несходные применения такого положения не будут затронуты.

(b) Настоящий приказ не предназначен и не создает никаких прав или выгод, материальных или процессуальных, подлежащих исполнению по закону или в соответствии с законом любой стороны против Соединенных Штатов, их департаментов, агентств или организаций, их должностных лиц, служащих или агентов, или любого другого лица.

(c) Ничто в настоящем приказе не должно толковаться как наносящее ущерб или иным образом затрагивающее:

полномочия, предоставленные законом исполнительному департаменту или учреждению, или его руководителю; или

функции Директора Управления по вопросам управления и бюджета, связанные с бюджетными, административными или законодательными предложениями.

(d) настоящий приказ осуществляется в соответствии с применимым законодательством и при условии наличия ассигнований.

Защита технологий

Этот план действий подробно описывает, как Соединенные Штаты должны разработать политику защиты технологий, чтобы обеспечить сохранение существующих преимуществ в технологических областях, применимых к национальной безопасности, но избежать удушения инноваций. Однако по мере того, как технологии dualuse становятся все более важными для национальной безопасности США, технологические преимущества сужаются, а иностранные усилия по приобретению американских ноу-хау и технологий увеличиваются, Соединенные Штаты также должны пересмотреть, как они могут защитить свою коммерческую и академическую экосистему от иностранной эксплуатации. Соединенные Штаты сталкиваются с

существенными проблемами в адаптации своего режима защиты технологий к угрозам, связанным с новыми технологиями двойного назначения, такими как искусственный интеллект (ИИ), не препятствуя свободному потоку торговли или открытой исследовательской среде, которые являются системными сильными сторонами США. Этот План действий предлагает реформы для (1) модернизации экспортного контроля и скрининга инвестиций и (2) защиты исследовательской среды США способами, совместимыми с национальной безопасностью США, коммерческими интересами и ценностями.

Модернизация экспортного контроля и скрининга инвестиций

То’ как правительство США регулирует доступ конкурентов к сложным американским технологиям с применением национальной безопасности, будет одной из главных проблем нынешней и будущей геоэкономической конкуренции. Соединенные Штаты должны модернизировать свои режимы экспортного контроля и проверки инвестиций, чтобы лучше решать проблемы, связанные с новыми технологиями двойного назначения, включая ИИ. Эти реформы необходимы для того, чтобы позволить правительству осуществлять политику защиты технологий таким образом, чтобы максимизировать их влияние на военный потенциал США. стратегические конкуренты и минимизировать любой последующий вред для американской промышленности.

Рекомендация: Четко сформулировать Общие принципы, которыми будут руководствоваться будущие политики США в области защиты технологий двойного назначения.

Правительство США должно четко сформулировать принципы, которыми будут руководствоваться будущие решения США в отношении политики защиты критических технологий. Это позволит проводить более последовательную и согласованную политику защиты технологий и обеспечит ясность для промышленности относительно того, как правительство намерено использовать эти инструменты регулирования в текущей конкурентной среде,

тем самым снижая неопределенность для американских предприятий. В настоящее время такой структуры не существует.

Действия для президента:

• Издать Исполнительный указ с изложением принципов, которыми будет руководствоваться политика США в области защиты технологий двойного назначения.

Президент должен издать Исполнительный указ, разъясняющий руководящие принципы, которыми будет руководствоваться политика США по защите критически важных технологий двойного назначения, включая ИИ. Исполнительный указ должен включать следующие руководящие принципы:

Американский технологический контроль не вытеснит инвестиции и инновации.

Стратегии США по продвижению и защите технологического лидерства США будут интегрированными и взаимоукрепляющими.

Соединенные Штаты будут благоразумно применять экспортный контроль к технологиям, связанным с ИИ, ориентируясь на отдельные контрольные точки и координируя политику с союзниками.

Соединенные Штаты расширят инвестиционный скрининг для защиты технологий, связанных с ИИ.

Укрепление потенциала США по проведению Эффективной Политики Защиты Технологий

Департаментам и ведомствам, ответственным за защиту американских технологий, не хватает организационного и технического потенциала для разработки и реализации эффективной политики по предотвращению передачи чувствительных к национальной безопасности компонентов новых технологий, таких как ИИ. Они страдают от недостатка технических талантов, необходимых для определения эффективной новой политики, и не имеют аналитического потенциала для эффективного проведения своей политики, особенно в отношении товаров двойного назначения. Заполнение этих пробелов в ключевых элементах Исполнительной власти-особенно в департаментах

торговли, Казначейства и государства-повысит способность правительства разрабатывать целевые меры экспортного контроля, которые оказывают наибольшее стратегическое воздействие и наносят наименьший ущерб конкурентоспособности США.

Действия для Министерства торговли:

• Назначить сеть ФФРРК и ОАРК в качестве общего технического ресурса по вопросам экспортного контроля.

Для углубления своей внутренней технической экспертизы Министерство торговли должно создать сеть в рамках существующих финансируемых из федерального бюджета научно-исследовательских и опытно-конструкторских центров (FFRDCs) и связанных с университетами научно-исследовательских центров (UARCs) для предоставления технической экспертизы всем департаментам и агентствам по вопросам, касающимся экспортного контроля за новыми технологиями. Эта сеть должна координироваться Министерством торговли и охватывать региональное распределение FFRDCS и UARCS, которые либо расположены в технологических центрах США, либо обладают значительным опытом в области новых технологий.

В качестве первого шага Министерству торговли следует определить РСФСР и ОАРК, обладающие существующим опытом в области новых технологий, рассматриваемых в целях экспортного контроля. За этим должна последовать просьба о финансировании в Бюджете Президента на 2022 финансовый год (FY) для поддержки и расширения работы FFRDCS и UARCs, сосредоточенных на экспортном контроле.

• Требовать, чтобы все новые правила защиты новых технологий согласовывались с существующими техническими консультативными группами, в состав которых входят внешние эксперты.

Министр торговли должен потребовать, чтобы Бюро промышленности и безопасности (БИС) запрашивало и получало отзывы о любых предлагаемых мерах контроля за новыми или основополагающими технологиями, включая предлагаемые правила и положения, от Технического консультативного

комитета по новым технологиям (ЭТТАК) и любых других соответствующих технических консультативных групп. Более частое и эффективное использование таких существующих консультативных комитетов обеспечило бы гибкую техническую экспертизу ключевых департаментов, помогло бы предотвратить публикацию контрпродуктивных мер контроля., и обеспечить, чтобы политики услышали точку зрения промышленности и научных кругов, прежде чем контроль вступит в силу.

Действия для Министерства торговли, казначейства и государства:

• Ускорить и автоматизировать процессы лицензирования экспорта и подачи заявок CFIUS.5

Министерство торговли и Министерство финансов должны сотрудничать с FFRDCS, UARCs и другими контрактными организациями для создания интегрированной интеллектуальной системы анализа заявок на экспортные лицензии и подачи заявок в Комитет по иностранным инвестициям в Соединенных Штатах (CFIUS). Эта система должна использовать ИИ для проведения предварительного анализа заявок и попытки оценить уровни риска до рассмотрения человеком. В ближайшей перспективе это поможет определить, какие операции являются очень низкорисковыми, а какие-очень высокорисковыми, чтобы помочь последующему человеческому анализу. В долгосрочной перспективе он может оказаться более точным, чем человеческий анализ, и принимать решения без участия человека, позволяя проводить точные, быстрые и менее трудоемкие обзоры.

• Поощрять союзников к проведению правовых реформ, разрешающих им осуществлять односторонний экспортный контроль и совершенствовать процедуры проверки инвестиций.

Государственные департаменты и министерства торговли должны настоятельно призвать всех союзников, которые еще не сделали этого, принять внутреннее законодательство для пересмотра своих режимов экспортного контроля, увеличения их бюрократического потенциала и предоставления им полномочий для осуществления одностороннего экспортного контроля. В

настоящее время многие союзники не имеют таких внутренних правовых полномочий и вместо этого передают все решения о регулировании многосторонним организациям, таким как Вассенаарские договоренности и Европейский союз. Эти реформы необходимы для того, чтобы позволить союзникам осуществлять целенаправленный, быстрый и эффективный экспортный контроль за новыми технологиями двойного назначения, которые быстро развиваются. Режимы защиты технологий в отношении глобально доступных продуктов настолько сильны, насколько сильны их самые слабые звенья, что требует сотрудничества США с союзниками и сильного регулирующего потенциала союзников. Это опирается на существующую работу, которая была продуктивной и должна быть продолжена с немедленным акцентом на страны, имеющие сильную внутреннюю формирующуюся технологическую базу и слабые режимы регулирования.7

Государственным департаментам и Казначейству следует активизировать усилия по расширению возможностей проверки инвестиций близких союзников и партнеров. Существующие усилия показали некоторый успех, но теперь требуют повышенной срочности, учитывая угрозы, с которыми сталкиваются союзники со стороны враждебного капитала, и желание США освободить некоторые фирмы в союзных странах от определенных требований CFIUS.8 Государство и Казначейство должны также регулярно обмениваться данными о структуре инвестиционных потоков в Соединенных Штатах и союзных странах, чтобы помочь союзным усилиям по блокированию хищнических инвестиций и проиллюстрировать характер угрозы.

• Обеспечить, чтобы ведомства, ответственные за экспортный контроль и политику проверки инвестиций, располагали достаточными ресурсами и техническим потенциалом.

Министерства торговли, Казначейства и государства должны обеспечить, чтобы ведомства, ответственные за разработку и осуществление положений об экспортном контроле и проверке инвестиций в отношении новых технологий, располагали достаточными ресурсами и имели достаточный технический

потенциал. Агентства должны полагаться на внешние источники, такие как FFRDCS, UARCs и консультативные советы, для получения глубокой технической экспертизы по конкретным технологиям. Однако они также должны обеспечить, чтобы подразделения, ответственные главным образом за управление политическими процессами, касающимися контроля за этими технологиями, располагали достаточным персоналом, ресурсами и базовым техническим потенциалом для того, чтобы идти в ногу с быстро меняющимися проблемами безопасности, связанными с технологиями двойного назначения.

Рекомендация: Определить «Новые» и «Основополагающие» Технологии, Которые Должны Контролироваться, как Того Требует Закон о реформе экспортного контроля 2018 года.

Закон о реформе экспортного контроля 2018 года (ECRA) и Закон о модернизации обзора рисков иностранных инвестиций 2018 года (FIRRMA) предназначены для пересмотра режимов экспортного контроля и скрининга инвестиций США, чтобы лучше приспособиться к новым технологиям. ECRA требует от Министерства торговли разработать регулярный, формальный межведомственный процесс для выявления «новых и основополагающих технологий, которые ... имеют важное значение для национальной безопасности Соединенных Штатов» и не контролируются иным образом. Любые такие технологии, идентифицированные Коммерцией, становятся предметом регулирования США. экспортный контроль и любые иностранные инвестиции в американскую компанию, которая «производит, проектирует, тестирует, производит, изготавливает или разрабатывает» одну или несколько таких технологий, должны быть рассмотрены CFIUS.10 Этот список должен отличаться от усилий в рамках предложенной Комиссией Национальной технологической стратегии (НТС) по определению новых технологий, имеющих ключевое значение для национальной конкурентоспособности и национальной безопасности США. Список ECRA должен быть более узко определен и сосредоточен только на конкретных технологиях, для которых необходим экспортный контроль, в то время как TCC и NTS должны

сосредоточиться на выявлении более широких технологий и конкретных платформ, в которых необходимо дальнейшее лидерство США.

Однако по состоянию на март 2021 года Министерство торговли еще не определило ни одной новой или основополагающей технологии, как это предписано ECRA. Хотя есть основания быть разумным в разработке этого списка, учитывая его последствия для промышленности США, а торговля сталкивается с законными ограничениями потенциала и ресурсов, масштабы задержки неприемлемы. Задержка вызвала двухпартийную критику, создала неопределенность для фирм, работающих в областях, которые можно было бы назвать новыми или основополагающими технологиями, и задержала способность правительства либо контролировать экспорт, либо, что более важно, получить представление о сделках, связанных с критическими технологиями, которые иначе не контролируются.

Определение этого списка технологий имеет решающее значение для того, чтобы позволить Соединенным Штатам полностью реализовать как EZRA, так и FIRRMA. Поскольку ECRA и FIRRMA структурированы, до тех пор, пока Министерство торговли не определит технологию, которая иначе не контролируется, как «развивающуюся и основополагающую» в рамках этого процесса обзора, за редкими исключениями CFIUS не может требовать от иностранных компаний раскрывать неконтролирующие инвестиции в американские технологические фирмы. Хотя Комиссия также рекомендует отказаться от использования CFIUS этого списка ECRA для обязательного раскрытия информации (см. Рекомендации по реформированию CFIUS для конкуренции новых технологий ниже), в настоящее время задержка Коммерции в выявлении таких технологий препятствует полному внедрению как ECRA, так и FIRRMA.

Меры для Министерства торговли:

• Поручить Бюро промышленности и безопасности разработать предлагаемые правила, содержащие первоначальные перечни как «новых», так и «основополагающих» технологий, к 31 декабря 2021 года.

Министр торговли должен поручить БМР к 31 декабря 2021 года совместно с американским межведомством разработать первоначальные версии списков «новых» и «фундаментальных» технологий. После 2021 года эти списки должны регулярно пересматриваться итеративным образом, чтобы соответствовать мандату ЕКРА по коммерции для постоянного совершенствования этих списков. В рамках этого итеративного процесса обзора коммерция также должна регулярно взаимодействовать с промышленностью по мере развития и развития технологий. Доработка первоначальных версий этих перечней, если они будут должным образом определены и определены, позволит контролировать критические технологии, разъяснить промышленности, как коммерция намерена внедрять ECRA, и обеспечить включение таких технологий в CFIUS.

Рекомендация: Реформировать CFIUS для конкуренции новых технологий CFIUS в настоящее время не предназначен для решения целого ряда угроз, с которыми сталкиваются Соединенные Штаты со стороны враждебного капитала со стороны стратегических конкурентов, таких как Китай и Россия. Министерство финансов имеет мало информации о российских и китайских инвестициях в американские развивающиеся технологические компании, поскольку заявки CFIUS по-прежнему в основном являются добровольными для неконтролируемых инвестиций в такие отрасли, как искусственный интеллект, полупроводники, квантовые вычисления и телекоммуникационное оборудование. Хотя ФИРРМА предприняла позитивные шаги по расширению полномочий CFIUS, она также оставила критические пробелы в режиме проверки инвестиций. Необходимы дополнительные шаги, чтобы CFIUS мог защитить чувствительные отрасли промышленности США от враждебного капитала, обеспечивая при этом непрерывный свободный поток капитала от надежных инвесторов из стран-союзников.

Действия для Конгресса:

• Внести поправки в разрешающее законодательство CFIUS, обязывающие конкурентов раскрывать CFIUS информацию об инвестициях в «чувствительные технологии».

Конгресс должен внести поправки в разрешающее законодательство CFIUS, чтобы обязать CFIUS подавать заявки на все неконтролирующие инвестиции из «стран, представляющих особый интерес», в «чувствительные технологии».» Комиссия рекомендует, чтобы законодательство:

Определить «страны, вызывающие особую озабоченность» как государства, на которые распространяются экспортные ограничения в соответствии с разделом 744.21 раздела Кодекса федеральных нормативных актов (Китай, Россия и Венесуэла), или любое государство, которое Государственный секретарь называет государством-спонсором терроризма (Иран, Северная Корея и Сирия).

Потребовать от Министерства финансов определить отдельный перечень «чувствительных технологий» для целей CFIUS. Только инвесторы из «стран, представляющих особый интерес», должны будут подавать заявки CFIUS на инвестиции в «чувствительные технологии.» Казначейство в настоящее время не имеет полномочий для расширения обязательных требований CFIUS к подаче заявок, которые связаны со списками технологий, контролируемых экспортом.

Обязательные заявки CFIUS от избранных конкурентов в более широком спектре чувствительных отраслей, таких как применение ИИ, полупроводников, квантовых вычислений и современного телекоммуникационного оборудования, позволят Казначейству лучше видеть российские и китайские инвестиции в американские фирмы в ключевых секторах. Это позволяет CFIUS работать с большей точностью и проницательностью и фокусировать внимание на самых рискованных инвестициях.

Кроме того, снятие привязки требований CFIUS к раскрытию информации от экспортного контроля признает, что существуют случаи, когда может быть целесообразно провести проверку инвестиций до введения экспортного контроля. Без этого изменения единственным способом повышения таких требований к раскрытию информации было бы введение экспортного контроля над целыми отраслями, что значительно затруднило бы торговлю.

Меры для Министерства финансов:

• Ускорить стандарты освобождения CFIUS для союзников и партнеров и создать быстрые пути для освобождения доверенных инвесторов.

Министерство финансов должно издать четкие указания относительно того, какую политику скрининга инвестиций должны проводить страны-союзники для достижения статуса CFIUSexempted. Четкое определение стандартов для механизмов проверки инвестиций в иностранных государствах, необходимых для освобождения инвесторов от CFIUS, создаст мощный стимул для союзных стран принять более сильные механизмы проверки против конкурирующего капитала. Чем скорее Казначейство предпримет это действие, тем большее влияние оно окажет на правила союзников. Казначейство должно уделять приоритетное внимание взаимодействию с партнерами по обмену разведывательными данными Five Eyes, Японией, Южной Кореей, Индией, Израилем, Сингапуром, Тайванем и Европейским союзом, чтобы обеспечить инвестиции союзных стран в американские высокотехнологичные фирмы.

Казначейство также должно издать новые правила, предусматривающие отказ для «доверенных инвесторов» из иностранных стран, которые имеют сильный послужной список одобрения CFIUS, чтобы освободить их от требований CFIUS или уменьшить их требования. В настоящее время не существует сертификации для инвесторов с надежным послужным списком, и CFIUS относится к иностранным инвесторам, которые подают заявку впервые, так же, как и к тем, которые уже подали заявку и были одобрены 100 раз. Создание такого отказа позволило бы CFIUS быстро отслеживать инвестиции

от низкорисковых, надежных инвесторов с сильной историей одобрения CFIUS, облегчая законные иностранные инвестиции и фокусируя ресурсы CFIUS на более высоких инвестициях.

Рекомендация: Использовать Целенаправленный экспортный контроль в отношении Ключевого оборудования для производства полупроводников

Хотя Комиссия считает, что экспортный контроль над алгоритмами ИИ, вероятно, будет неэффективным, учитывая их широкую доступность и коммерческое использование, экспортный контроль над конкретными аппаратными компонентами способен ограничить возможности ИИ конкурентов с помощью приложений национальной безопасности и замедлить их продвижение. Политики должны быть благоразумны в применении такого контроля, поскольку радикальный контроль за полупроводниками общего назначения, вероятно, нанесет существенный ущерб полупроводниковой промышленности США и может иметь чистый негативный эффект на общую экономику США. конкурентоспособность в микроэлектронике. Однако целенаправленный контроль над ключевыми компонентами, которые производят только Соединенные Штаты—или Соединенные Штаты и небольшая группа близких союзников—и которые необходимы для передовых оборонных приложений, может оказать значительное стратегическое воздействие при относительно минимальных затратах.

Основной целью такого контроля должно быть отборное высокотехнологичное полупроводниковое производственное оборудование (МСП), необходимое для производства высококачественных чипсетов, в частности фотолитографического оборудования. Китай является крупнейшим в мире импортером МСП, на долю которого приходится 29% мирового импорта с 2014 по 2018 год, и ни одна из крупнейших или наиболее сложных фирм-производителей МСП не находится в Китае. Одновременно с осуществлением мер контроля, Соединенные Штаты также должны финансировать усилия по приоритизации внутренней разработки и производства инструментов и

компонентов МСП, необходимых для производства чипов в масштабе 3-нм узла и за его пределами.

Меры для Министерства торговли и государственного управления:

• Согласовать политику экспортного контроля Соединенных Штатов, Нидерландов и Японии с целью ограничения экспорта высокотехнологичных МСП в Китай, включая оборудование для иммерсионной литографии EUV и ArF.

Государственные департаменты и министерства торговли должны работать над согласованием политики экспортного контроля Соединенных Штатов, Нидерландов и Японии в отношении высокотехнологичных МСП, в частности оборудования для экстремальной ультрафиолетовой литографии (EUV) и оборудования для иммерсионной литографии на основе фторида аргона (ArF), которое способно производить чипы на узле 16 нм и ниже. Всем трем государствам следует установить политику предполагаемого отказа в выдаче экспортных лицензий на экспорт такого оборудования в Китай. Это должно включать инструменты сканера EUV, а также специализированные компоненты для этих инструментов, например, резистивные обрабатывающие инструменты и источники света EUV, зеркала и лазерные усилители. Если такой контроль будет эффективным, китайскому правительству будет трудно развивать собственные передовые технологии производства полупроводников и ухудшать свои передовые технологии производства, усложняя ремонт оборудования. В сочетании с возвратным инвестиционным налоговым кредитом для продвижения лидерства США в области полупроводников, рекомендованным в главе 13 настоящего доклада, это будет способствовать дальнейшему развитию предложенной Комиссией стратегии США. политическая цель-опередить Китай на два поколения в области разработки и производства ультрасовременной микроэлектроники.

• Оценить эффективность существующего экспортного контроля США за МСП в полупроводниковой промышленности Китая и оценить, является ли

целевой контроль за дополнительным оборудованием жизнеспособным и необходимым.

Министерствам торговли и Госдепартамента следует оценить эффективность существующего в США экспортного контроля за МСП в отношении местной передовой полупроводниковой промышленности Китая. В ожидании результатов этого обзора и того, согласятся ли Нидерланды, и Япония согласовать меры контроля, связанные с погружным оборудованием EUV и ArF, Соединенные Штаты могли бы впоследствии рассмотреть вопрос о мерах контроля в отношении дополнительных контрольных точек МСП. Если существующие меры контроля не смогли замедлить развитие Китаем передовых производственных мощностей, Соединенные Штаты могли бы рассмотреть вопрос о введении контроля над другими целевыми узлами оборудования, контролируемыми фирмами в союзных странах, такими как инструменты для травления атомного слоя совместно с Японией и Соединенным Королевством.

Рекомендация: Использовать экспортный контроль конечного использования для предотвращения злонамеренного использования ИИ. Экспортный контроль, ограничивающий передачу товаров двойного назначения для конкретных конечных целей, не будет эффективным в предотвращении передачи технологий определенным противникам, но он все же может сыграть определенную роль в предотвращении вовлечения американских фирм и технологий в нарушения прав человека. Для специфического, высококлассного оборудования двойного назначения, способного облегчить использование ИИ, которое допускает нарушения прав человека, например, массовое наблюдение, американские фирмы должны быть обязаны удостоверить, что это оборудование не будет использоваться для конкретных гнусных целей, и вести журналы своих операций. Контроль конечного использования и требования к отчетности не будут существенно задерживать продажи и представлять собой более низкий барьер для торговли по сравнению с контролем на основе списков. Требование от компаний

самосертификации и самоотчета может помешать американским фирмам сознательно допускать плохое поведение за рубежом.

Меры для Министерства торговли:

• Внедрить контроль конечного использования и требования к отчетности для предотвращения использования высококачественных американских чипов искусственного интеллекта при нарушениях прав человека.

Министерство торговли должно внедрить контроль конечного использования высококачественных чипов ИИ, разработанных или изготовленных в США, для использования в приложениях массового наблюдения и установить требования к отчетности о продажах таких чипов в Китай. Элементы управления должны быть нацелены только на очень высококачественные или специализированные чипы, такие как специальные высокопроизводительные графические процессоры, ASIC или FPGA, которые превышают определенный порог высокой производительности. Коммерция, по необходимости, обновит этот порог, поскольку чипы продолжают улучшаться.

Любая фирма, которая продает такие чипы в Китай, должна подтвердить, что чипы не будут использоваться для каких-либо определенных нарушений прав человека. Фирмы, которые продают такие чипы, также должны предоставлять ежеквартальные отчеты в BIS с перечислением всех продаж чипов, в каком количестве и какой компании. Это облегчит правительству США отслеживание чипов, которые, скорее всего, будут способствовать неправомерному использованию ИИ, и удержит компании от продажи чипов компаниям, которые, как они знают, занимаются таким поведением.

Защита исследовательской среды США

Соединенные Штаты нуждаются во всесторонних и обеспеченных ресурсами межведомственных мерах по противодействию враждебным угрозам для их исследовательской среды, особенно со стороны Китая. Усилия должны подкрепляться технически грамотным сбором, анализом и распространением разведданных об угрозах в научно-техническом (Научно-техническом) пространстве. Многообещающие шаги были предприняты через Национальную

целевую группу по контрразведке и Управление научно-технической политики. Однако крайне важно целостно улучшить то, как правительство позиционирует себя и оснащает исследовательское сообщество в академических кругах и частном секторе—для противодействия угрозам и поддержания целостности открытых исследований.

Рекомендация: Создание потенциала для защиты целостности исследовательской среды США

Действия для Конгресса:

• Принять измененную версию Закона о защите научных исследований.

Конгресс должен принять Закон о защите академических исследований (ARPA) с изменениями, которые будут предписывать и осуществлять стандартизацию процессов предоставления грантов между федеральными агентствами, финансирующими исследования.29

АРПА учредит Национальную комиссию по защите научных исследований; создаст информационно-координационный центр с открытым исходным кодом по вопросам иностранных угроз академическим кругам под надзором директора национальной разведки; улучшит руководство Государственными департаментами и коммерческими ведомствами по вопросам экспортного контроля; и разработает информационно-пропагандистскую стратегию Федерального бюро расследований (ФБР) для содействия обмену информацией об угрозах академическому сообществу.

Предлагаемое изменение будет предусматривать разработку и внедрение единого процесса подачи заявок и базы данных во всех исполнительных органах, предоставляющих гранты на НИОКР. Это позволило бы обеспечить эффективный надзор со стороны агентств, предоставляющих гранты, автоматизировать аудит и поддержать следственные действия федеральных правоохранительных органов.

• Создать спонсируемую правительством независимую организацию, ориентированную на добросовестность исследований.

Конгресс должен разрешить спонсорство исследовательского центра, связанного с университетом (UARC), чтобы действовать в качестве центра передового опыта в области целостности исследований и предоставлять информацию и консультации по вопросам безопасности исследований.

Организация должна ликвидировать разрыв между правительством и научно-исследовательскими институтами академического и частного секторов и снизить барьеры для научно-исследовательских организаций, препятствующие независимому проведению комплаенс-анализа и обоснованной оценки рисков.

Мандат ОАРК должен заключаться в следующем:

Ведение материалов с открытым исходным кодом для проведения университетской проверки международного взаимодействия и управления рисками, включая базы данных и инструменты оценки рисков;

Предоставлять индивидуальные рекомендации исследовательским организациям для поддержки принятия решений;

Проводить комплексные исследования и регулярные отчеты о состоянии иностранного влияния на исследования США;

Проведение независимых исследований по вопросам добросовестности исследований;

Разработка учебных материалов и инструментов для научно-исследовательских институтов США для создания ежегодных инициатив по обучению и соблюдению требований; и Управление диалогом с заинтересованными сообществами и предоставление площадки для обмена информацией.

Меры в отношении директора национальной разведки:

• Укрепление каналов обмена информацией с исследовательским сообществом.

Совместно с информационно-координационным центром по разведке с открытым исходным кодом, связанным с иностранными угрозами академическим кругам, руководимым законодательством ARPA, директор

национальной разведки должен поддерживать расширение обмена информацией и разведывательными данными с назначенными сотрудниками исследовательских организаций для обмена полезной информацией о конкретных угрозах. Это даст организациям возможность оперативно принимать меры по снижению рисков.

Рекомендация: Координировать усилия по защите исследований на международном уровне с союзниками и партнерами.

Соединенные Штаты должны создать коалицию стран-единомышленников, приверженных принципу открытых фундаментальных исследований и связанным с ними ценностям честности исследований, отодвинув на второй план страны и организации, которые не придерживаются ценностей, обеспечивающих основу для международного сотрудничества в области инноваций и науки.

Меры для Управления научно - технической политики:

• Содействовать международному диалогу по вопросам защиты и добросовестности научных исследований.

Управление научно-технической политики через Национальный совет по науке и технике должно работать в координации с Управлением научно-технического сотрудничества Государственного департамента и Управлением Советника по науке и технике в целях содействия дискуссиям с единомышленниками-союзниками и партнерами, направленным на смягчение пагубного академического сотрудничества с ассоциированными с Народно-освободительной армией Китая (НОАК) и другими организациями высокого риска. Это должно включать в себя создание ежегодной встречи соответствующих министров образования, науки и промышленности для углубления сотрудничества в области исследований и координации по вопросам, связанным с интеллектуальной собственностью и безопасностью исследований.

Меры для Министерства юстиции:

• Укрепление центров обмена информацией.

Министерство юстиции (Минюст) и ФБР в координации с партнерами по разведывательному сообществу должны укреплять каналы обмена информацией об угрозах и передовой практике защиты научных исследований и координировать многосторонние меры реагирования для обеспечения безопасности научных исследований.

Действия для Государственного департамента:

• Укрепление глобальных норм, связанных с обязательством проводить открытые фундаментальные исследования.

Посредством международного диалога по вопросам безопасности научных исследований и связанной с этим дипломатии Государственный департамент должен укреплять глобальные нормы, касающиеся приверженности открытым фундаментальным исследованиям,31 как это описано в Соединенных Штатах в Директиве о принятии решений по национальной безопасности (NSDD)-189, Национальной политике передачи научной, технической и инженерной информации.

Рекомендация: Усилить поддержку научно-исследовательских институтов в области кибербезопасности

Защита исследовательских данных и интеллектуальной собственности от киберугроз является, пожалуй, самым важным и действенным уровнем безопасности для американской научно-исследовательской среды. Это особенно верно для ИИ, когда кража обучающих данных или обученных моделей по существу обеспечивает злоумышленникам доступ к конечному продукту. Федеральные инвестиции в приоритетные новые области исследований в области технологий, такие как ИИ, должны сопровождаться требованием и поддержкой для учрежденийбудь то академический или частный сектор осуществлять меры кибербезопасности, которые адекватно защищают исследовательские данные от киберугроз.

Действия для американских грантодающих агентств:

• Стимулирование стандартов кибербезопасности и передовой практики для исследовательских учреждений, получающих гранты.

Американские агентства, предоставляющие гранты,должны предоставлять исследовательским учреждениям стимулы для обеспечения необходимой практики, основанной на существующей системе кибербезопасности NIST, а также процессов управления для защиты конфиденциальных исследовательских данных.

Структуры отчетности и информационные потоки научно-исследовательских учреждений должны быть структурированы таким образом, чтобы поднять кибербезопасность как важнейший вопрос для высшего руководства и облегчить внутренние проверки и аудиты. Это включает в себя осведомленность высшего руководства о киберугрозах, оценку рисков и активные превентивные меры.

Американские грантодатели должны предоставлять стимулы для исследовательских институтов, которые демонстрируют приверженность стандартам и передовой практике кибербезопасности.

Университеты, исследовательские институты и другие получатели федерального финансирования исследований должны периодически демонстрировать, что они придерживаются лучших практик в области кибербезопасности. Для лабораторий, находящихся в государственной собственности и спонсируемых государством, соблюдение передовой практики, такой как требование шифрования критически важных данных в состоянии покоя и при транспортировке, должно быть санкционировано и проверяться на регулярной основе.

• Поддержка расширения обмена информацией.

Исследовательские учреждения, получающие федеральные исследовательские доллары, которые еще не участвуют в них, следует поощрять к присоединению к Информационно-аналитическому центру научно-образовательных сетей (REN-ISAC) или альтернативному ISAC, через который они могут обмениваться информацией об угрозах и смягчении их последствий, пользоваться автоматизированными инструментами обмена угрозами и иметь доступ к услугам коллегиальной оценки для укрепления позиций безопасности.

Аналогичным образом, научно-исследовательские учреждения следует информировать и поощрять к тому, чтобы они пользовались услугами по кибербезопасности, предлагаемыми Агентством по кибербезопасности и инфраструктурной безопасности Министерства внутренней безопасности (CISA), включая автоматизированный обмен показателями35 и расширенные услуги по кибербезопасности.

Действия Федерального бюро расследований:

• Делитесь информацией об угрозах в режиме реального времени с исследовательскими институтами.

Отдел кибербезопасности ФБР должен тесно сотрудничать и обмениваться своевременной анонимной информацией об угрозах с REN-ISAC и исследовательскими институтами, чтобы помочь им принять активные меры по противодействию кибератакам и смягчению уязвимостей.

Меры для Министерства внутренней безопасности:

• Поддержка исследований в области обмена информацией о кибербезопасности, аналогичного обмену информацией о критической инфраструктуре.

Министерство внутренней безопасности, CISA и Национальный центр интеграции кибербезопасности и Коммуникаций37 должны поддерживать уровень обмена информацией с исследовательскими институтами, как они это делают с критической инфраструктурой и ISAC финансовых услуг.

Меры для Управления научно - технической политики:

• Поддержка безопасного хранения данных.

OSTP должна предоставлять университетам коммерческие облачные кредиты для создания возможности поддержки безопасного хранения данных для исследовательских групп и лабораторий, проводящих работы, которые, как известно, представляют большой интерес для иностранных противников. Это дало бы университетам возможность защищать свои чувствительные исследования таким образом, чтобы это не требовало значительных капиталовложений.

Рекомендация: Противодействие Программам Привлечения Иностранных Талантов

Китай использует программы привлечения иностранных талантов для достижения «высокого уровня» экспертов в области ИИ. Вместо того чтобы проводить законную конкуренцию за научные таланты с помощью привлекательных предложений о работе, китайские планы найма талантов разрабатываются таким образом, чтобы противоречить американским нормам честности исследований, нарушать правила раскрытия информации и создавать векторы для передачи технологий. По оценке ФБР и разведывательного сообщества, «участников часто побуждают передавать Китаю исследования, которые они проводят в Соединенных Штатах, а также другую конфиденциальную информацию, к которой они могут получить доступ.» Существует настоятельная необходимость в укреплении стандартов, касающихся раскрытия информации о конфликтах интересов и обязательств, а также в создании механизмов, обеспечивающих более высокий уровень прозрачности и подотчетности. Это относится к индивидуальной прозрачности исследователей и институциональной подотчетности, а также к правительству в выявлении проблемных аффилиаций и обеспечении соблюдения стандартов. В настоящее время американские грантодатели не имеют общих процессов, координации и механизмов соблюдения, обеспечивающих такой уровень прозрачности и эффективного надзора.

Меры для Управления научно - технической политики:

• Стандартизация процессов подачи заявок на получение грантов и их регистрации.

Управление научно-технической политики (ОСТП) в координации с Управлением по вопросам управления и бюджета должно предоставлять консультации и координировать деятельность исполнительной власти в целях обеспечения единообразия процессов подачи заявок на гранты и регистрации в федеральных агентствах, финансирующих внешние исследования.

ОСТП должна консультировать и координировать свои действия с агентствами, чтобы обеспечить принятие агентствами общегосударственного стандарта документации по грантовым предложениям, требующего машиночитаемых форматов, облегчающих автоматизацию выявления мошенничества. Это позволило бы обеспечить эффективный надзор со стороны агентств, предоставляющих гранты, автоматизировать аудит и поддержать следственные действия федеральных правоохранительных органов.

Действия для Конгресса:

• Операции по соблюдению мандатов и ресурсов.

Конгресс должен потребовать и предоставить ресурсы американским грантодающим агентствам для поддержания комплаенс-операций, которые могут обеспечить соблюдение стандартизированных мер раскрытия информации и подотчетности. Благодаря периодической проверке и мониторингу учреждения, предоставляющие гранты, могут обеспечить уровень подотчетности для обеспечения соблюдения политики раскрытия информации и защиты.

• Внести изменения в Закон о регистрации иностранных агентов.

Конгресс должен внести поправки в Закон о регистрации иностранных агентов (FARA), обязывающие любое физическое или юридическое лицо, участвующее в наборе граждан США для участия в программе иностранных талантов, регистрироваться в качестве иностранного агента. Это требует от Конгресса добавить в законодательство новую категорию деятельности.

Действия для Министерства юстиции:

• Обновить правила подачи заявок в поддержку измененного FARA.

Если Конгресс внесет поправки в законодательство FARA, как это было предложено выше, Министерство юстиции в своих имплементационных правилах должно определить конкретную информацию, требуемую от лиц, участвующих в наборе иностранных талантов для программ, чтобы обеспечить правительству США надлежащую видимость деятельности по набору талантов иностранных стран в Соединенных Штатах.

Регламент Министерства юстиции должен включать методы обжалования отдельными лицами и организациями решения о том, что они подлежат регистрации в соответствии с настоящим расширением FARA.

• Публично выявлять базирующиеся в США организации и доверенные лица иностранных правительств, которые служат в качестве рекрутинговых сетей, платформ или брокеров.

Чтобы помочь повысить осведомленность исследователей и научно-исследовательских институтов и повысить прозрачность, федеральные правоохранительные органы и другие соответствующие ведомства должны выявлять организации, участвующие в деятельности по набору иностранных талантов, и требовать их регистрации через FARA (если в нее будут внесены поправки).

Эти усилия должны сопровождаться соответствующим апелляционным процессом для организаций, оспаривающих необходимость регистрации с точки зрения идентификации.

Рекомендация: Ограничить сотрудничество с аффилированными с НОАК лицами и организациями

Университеты и исследовательские лаборатории, связанные с НОАК, направляют персонал за границу с общей целью получения знаний, которые могут непосредственно питать приоритеты оборонных исследований и разработок. Приезжие ученые или студенты из учреждений НОАК часто преуменьшают свои связи с военными или намеренно скрывают принадлежность, используя альтернативные, внешние названия для своих родных учреждений, которые не упоминают военные или оборонные мандаты.

Правительство должно принять меры путем назначения учреждений, вызывающих озабоченность, и усиленной проверки виз, чтобы помочь университетам в оценке рисков, связанных с исследовательским сотрудничеством, став эффективным партнером в защите целостности исследований.

Меры в отношении директора национальной разведки:

• Создать базу данных с открытым исходным кодом организаций, которые имеют историю ненадлежащей передачи технологий, кражи интеллектуальной собственности или кибершпионажа.

Директор Национальной разведки в координации с партнерами по правоохранительным органам должен создать доступную для запросов базу данных академических учреждений и других организаций, которые имеют историю ненадлежащей передачи технологий, кражи интеллектуальной собственности или кибершпионажа. Этот ресурс должен служить исследовательскому сообществу и информировать исследовательские организации об оценке рисков при заключении соглашений о сотрудничестве. Он будет представлять собой экспансивный, открытый взгляд на исследовательские институты, вызывающие озабоченность, противодействуя попыткам скрыть военную принадлежность путем принятия безобидных институциональных псевдонимов.

Это должно сопровождаться соответствующим апелляционным процессом для организаций, оспаривающих их включение в базу данных.

Действия для президента:

• Ограничить въезд исследователей с военной и разведывательной принадлежностью из стран, вызывающих озабоченность.

Президент должен издать распоряжение Государственному секретарю и министру внутренней безопасности о введении требования о специальном пересмотре виз для студентов высших учебных заведений и исследователей, имеющих связи с научно-исследовательскими учреждениями, связанными с иностранными военными и разведывательными организациями указанных стран, представляющих интерес.

Это должно сочетаться со штрафами, которые запрещают въезд любым заявителям на визу, обнаружившим, что они намеренно скрывают свою институциональную принадлежность.

Действия для Государственного департамента:

• Специальные меры по обзору ресурсов.

Консульские сотрудники должны быть обеспечены надлежащей подготовкой, справочными ресурсами, аналитической поддержкой и временем для проведения специального обзора.

Защита технологии

Проект Исполнительного Указа об экспортном контроле о принципах, определяющих политику США в области защиты технологий двойного назначения

В соответствии с полномочиями, предоставленными мне как Президенту Конституцией и законами Соединенных Штатов Америки, а также в целях содействия инновациям и лидерству США в области новых и основополагающих технологий при одновременной защите национальной безопасности США, настоящим приказывается следующее:

Раздел 1. Политика. Политика Соединенных Штатов заключается в том, что механизмы экспортного контроля и проверки инвестиций должны использоваться целенаправленными, четко определенными и стратегическими способами для защиты национальной безопасности США в рамках более широкой политики поощрения инноваций и лидерства США в новых и основополагающих технологиях, включая технологии двойного назначения, такие как искусственный интеллект (ИИ).

Соединенные Штаты должны быть целенаправленными и дискретными в осуществлении экспортного контроля за новыми технологиями двойного назначения, такими как ИИ. Для обеспечения максимальной эффективности и минимизации негативного воздействия на промышленность США правительство США должно руководствоваться следующими принципами:

(1) Принцип первый: Экспортный контроль Не может вытеснить Инвестиции и инновации. Политика защиты технологий направлена на то, чтобы замедлить преследование и развитие ключевых стратегических технологий США в целях национальной безопасности, а не остановить их на своем пути. Соединенные Штаты должны развивать инвестиции в эти

технологии через прямое федеральное финансирование или изменения в нормативной среде, чтобы сохранить существующие преимущества США.

(2) Принцип Второй: Стратегии США по Продвижению и Защите Технологического Лидерства США Должны Быть Интегрированы. Стратегия США по защите новых технологий, включая, но не ограничиваясь ИИ, должна быть интегрирована с целенаправленными усилиями по продвижению американского лидерства в таких технологиях. Принимая решение о введении контроля, Соединенные Штаты должны одновременно рассмотреть политику стимулирования внутренних исследований и разработок (НИОКР) в ключевых отраслях, чтобы частично компенсировать возникающие издержки для американских фирм, создать альтернативные глобальные рынки или стимулировать новые инвестиции для укрепления США. промышленное положение.

(3) Принцип третий: Экспортный контроль должен быть Целенаправленным, Стратегическим и Скоординированным с союзниками. Разрабатывая новые меры экспортного контроля в отношении широко распространенных технологий двойного назначения, таких как ИИ, Соединенные Штаты должны проявлять осторожность и избирательность при осуществлении экспортного контроля. Чтобы обеспечить максимальную эффективность и минимизировать негативное воздействие на промышленность США, правительство США должно руководствоваться следующим трехчастным тестом:

a. Экспортный контроль должен быть целенаправленным, четко определенным и сфокусированным на узких точках, где он будет оказывать стратегическое воздействие на возможности национальной безопасности конкурентов, но меньшие последствия для промышленности США.

b. Экспортный контроль должен иметь четкую стратегическую цель, направленную на сдерживание конкурентов от следования путями, которые угрожают интересам национальной безопасности США, и учитывать

прогнозируемые затраты и сроки для конкурентов, чтобы создать внутреннюю альтернативу.

c. Экспортный контроль должен быть согласован с ключевыми союзниками США, которые также способны производить данную технологию, чтобы эффективно ограничить поставки противникам, а также предотвратить обстоятельства, при которых односторонний контроль отрезает доступ США на рынок, но конкуренты могут покупать ту же технологию у других стран.

(4) Принцип четвертый: Соединенные Штаты будут благоразумно использовать экспортный контроль, но расширят контроль за инвестициями в критические и новые технологии. В то время как широкий и широкий экспортный контроль над ИИ и другими новыми технологиями двойного назначения может привести к значительному удару по американской промышленности, что нанесет ущерб общей стратегической конкурентоспособности США, инвестиционный скрининг открывает возможности для принятия более активного подхода к регулированию при минимизации рисков для американской промышленности. При условии, что Соединенные Штаты могут продолжать оперативно одобрять доброкачественные сделки, усиление скрининга инвестиций представляет значительный потенциал для притупления в отношении передачи технологий.

Цель.

В 2018 году Конгресс принял Закон о реформе экспортного контроля 2018 года (ECRA) и Закон о модернизации системы снижения рисков иностранных инвестиций 2018 года (FIRRMA), чтобы предоставить правительству США дополнительные механизмы контроля экспорта и скрининга инвестиций. Правительство США должно предпринять шаги, чтобы обеспечить частному сектору и иностранным правительствам ясность в отношении применения этих законов к новым и основополагающим технологиям и укрепить национальную безопасность США в этом процессе.

Создание.

Межведомственной целевой группы по новым и основополагающим технологиям. (a) В соответствии с разделом 1758 ECRA настоящим учреждается Межведомственная целевая группа по новым и основополагающим технологиям (Task Force) для выявления новых и основополагающих технологий, которые имеют важное значение для национальной безопасности Соединенных Штатов и не являются критическими технологиями, описанными в пунктах (i) - (v) статьи 50 U. S. C. 4565(a)(6)(A).

(b) Целевая группа возглавляется Министром торговли (Председателем) и состоит из старших должностных лиц следующих исполнительных департаментов и учреждений (учреждений), назначаемых руководителями этих учреждений:

(i) Государственный департамент;

(ii) Департамент казначейства;

(iii) Министерство обороны;

(iv) Министерство энергетики; и

(vi) такие другие учреждения, которые могут быть назначены Председателем или Председателем.

(c) Председатель назначает должностное лицо старшего уровня Министерства торговли в качестве Исполнительного директора Целевой группы, которое отвечает за регулярный созыв и руководство совещаниями Целевой группы, определение ее повестки дня и руководство ее работой по выполнению ее функций в соответствии с настоящим Приказом в координации с БИС в Министерстве торговли.

Функции Целевой группы.

(a) Целевая группа проводит регулярные совещания для выявления новых и основополагающих технологий, имеющих важное значение для национальной безопасности Соединенных Штатов, в целях установления, в соответствующих случаях, механизмов экспортного контроля и проверки инвестиций, связанных с этими технологиями.

(b) в течение 120 дней Целевая группа завершит составление перечней новых и основополагающих технологий в соответствии с разделом 1758 ECPA. После этого Министр торговли издает предлагаемые правила по новым и основополагающим технологиям и оперативно приступает к изданию окончательных правил по завершении периода уведомления и комментариев.

(c) Целевая группа рассматривает перечни новых и основополагающих технологий и вносит необходимые поправки не менее чем на ежегодной основе.

Раздел 5. Процесс выявления новых и основополагающих технологий.

(a) при выявлении новых и основополагающих технологий в соответствии с настоящим Приказом Целевая группа рассматривает информацию из различных источников, включая:

общедоступная информация;

секретная информация, включая соответствующую информацию, предоставленную директором национальной разведки;

информация, касающаяся обзоров и расследований сделок, проводимых Комитетом по иностранным инвестициям в Соединенных Штатах в соответствии с 50 U. S. C. 4565; и

информация, представленная консультативными комитетами, учрежденными Секретарем для консультирования Заместителя министра торговли по вопросам промышленности и безопасности по вопросам контроля в соответствии с Правилами управления экспортом, включая Технический консультативный комитет по новым технологиям (ЭТТАК).

(b) при выявлении новых и основополагающих технологий в соответствии с настоящим

Приказом Целевая группа принимает во внимание:

развитие новых и основополагающих технологий в зарубежных странах;

влияние экспортного контроля, введенного в соответствии с настоящим разделом, на развитие таких технологий в Соединенных Штатах;

эффективность экспортного контроля, введенного в соответствии с настоящим разделом в целях ограничения распространения новых и основополагающих технологий в зарубежных странах; и

политика и принципы, отраженные в разделе 1 настоящего Приказа.

Раздел 6. Улучшение координации с Консультативными группами экспертов. (a) Министр торговли проводит обзор существующих технических консультативных комитетов (ТАК) в Министерстве торговли, включая ЭТТАК, для обеспечения того, чтобы каждый ТАК состоял из представителей промышленности и научных кругов, обладающих глубокими предметными знаниями, для оценки необходимости экспортного контроля за новыми и основополагающими технологиями.

(b) Министр торговли в качестве Председателя Целевой группы обеспечивает, чтобы Целевая группа запросила и получила обратную связь от ЕТТАС и других соответствующих ТАС в Министерстве торговли по тексту любого предлагаемого или окончательного правила о новых или основополагающих технологиях до опубликования такого правила.

(c) Министр торговли обеспечивает, чтобы старшим должностным лицам Государственных департаментов и Казначейства предоставлялся доступ наблюдателей без права голоса на все заседания ЭТТАК.

Совершенствование международной координации в области экспортного контроля за оборудованием для производства полупроводников.

В течение 180 дней Государственный секретарь в консультации с Министром торговли и Министром обороны организует многостороннее взаимодействие с высокопоставленными представителями Японии, Нидерландов и, если это будет сочтено целесообразным, других союзников и партнеров США, производящих полупроводниковое производственное оборудование (МСП), включая оборудование для литографии EUV и оборудование для иммерсионной литографии ArF, перечисленные в Вассенаарских договоренностях или определенные Целевой группой. Целью этой встречи будет согласование политики лицензирования экспорта в сторону

предполагаемого отказа в выдаче экспортных лицензий на экспорт оборудования для производства полупроводников в Китай. Государственный секретарь представляет доклад Президенту в течение 60 дней после заседания:

(i) экспортируют ли в настоящее время союзники и партнеры США такое оборудование в Китай;

(ii) какие шаги должна предпринять каждая страна, производящая такое оборудование, для обеспечения того, чтобы ее режим регулирования соответствовал режиму Соединенных Штатов, и ее готовность предпринять эти шаги; и

(iii) существуют ли дополнительные возможности для укрепления международного сотрудничества в области экспортного контроля в отношении тех же товаров, которые согласуются с политикой и принципами, отраженными в разделе 1 настоящего Приказа.

Привлечение технических экспертов для проведения обзора экспортного контроля.

(a) Министр торговли в консультации с министрами финансов и обороны создает сеть в рамках существующих финансируемых из федерального бюджета научно-исследовательских и опытно-конструкторских центров (FFRDCs) и Связанных с университетами научно-исследовательских центров (UARCs) для предоставления технических экспертных знаний всем департаментам и учреждениям по вопросам, касающимся экспортного контроля и проверки инвестиций, связанных с новыми и основополагающими технологиями. Сеть должна охватывать региональное распределение FFRDCS и UARCS, расположенных в районах Соединенных Штатов с концентрацией технологического опыта в новых и фундаментальных технологиях.

(b) Лица, отобранные для участия в сети, должны в режиме реального времени вносить технический вклад во все обсуждения политики в области экспортного контроля и рассмотрения заявок на получение лицензий на экспортный контроль, включая обсуждения Целевой группы, проводимые в соответствии с EO 12981 или последующим приказом, а также любые другие

межведомственные обсуждения политики, касающиеся экспортного контроля, а также процессы проверки инвестиций Комитета по иностранным инвестициям в Соединенных Штатах (CFIUS).

Автоматизация экспортного контроля и проверки инвестиций.

Министры торговли и Казначейства поручают вышеупомянутой сети изучить вопрос об использовании систем на основе ИИ для оказания помощи в оценке заявок на получение лицензий на экспортный контроль и заявок CFIUS и представляют Президенту доклад об использовании систем на основе ИИ для таких целей в течение 180 дней. Настоящий отчет должен включать оценку:

(i) каким образом системы, основанные на ИИ, могут помочь существующим процессам обзора;

(ii) может ли включение таких систем повысить точность и скорость процессов обзора;

(iii) располагают ли соответствующие департаменты и учреждения достаточным количеством и качеством данных для подготовки систем обзора на основе искусственного интеллекта, и каким образом можно улучшить существующие данные;

(iv) какая информационно-технологическая инфраструктура внутри соответствующих департаментов и учреждений нуждается в совершенствовании для полного использования таких систем; и

(iv) приблизительные сроки и стоимость развертывания системы или систем, а также прогнозируемая экономия в год в рабочих часах после развертывания.

Общие положения. (a) Ничто в настоящем Приказе не должно толковаться как наносящее ущерб или иным образом затрагивающее:

(i) полномочия, предоставленные законом, постановлением, Указом или Распоряжением Президента исполнительному департаменту, агентству или его руководителю; или

(ii) функции Директора Управления по вопросам управления и бюджета, связанные с бюджетными, административными или законодательными предложениями.

(b) настоящий приказ исполняется в соответствии с применимым законодательством и при условии наличия ассигнований.

(c) Настоящий приказ не предназначен и не создает каких-либо прав или выгод, материальных или процессуальных, подлежащих исполнению по закону или по справедливости любой стороной в отношении Соединенных Штатов, их департаментов, агентств или организаций, их должностных лиц, служащих или агентов или любого другого лица.

Благоприятный Международный Технологический Заказ

Этот план действий подробно описывает всеобъемлющую стратегию продвижения интересов США вместе с союзниками и партнерами для формирования благоприятного международного технологического порядка, победы в технологической конкуренции против авторитарных государств и продвижения инноваций и внедрения искусственного интеллекта (ИИ) по всему миру для продвижения ценностей свободного и открытого общества. Этот План действий также предлагает реформы для переориентации внешней политики США и Государственного департамента на конкуренцию великих держав в цифровую эпоху.

Рекомендация: Разработать Международную научно-техническую стратегию

Международная научно-техническая стратегия (МСТ) поможет координировать новую технологическую политику в рамках правительства и с нашими ближайшими союзниками и партнерами; применять инструменты иностранной помощи, технического опыта и руководства, а также финансирования и инвестиций в целях развития; а также способствовать совместным НИОКР. МСТ должны служить международным компонентом Национальной технологической стратегии (НТС) и обеспечивать организационную основу для проведения внешней политики США в

отношении новых технологий. ИСТ должны сосредоточиться на четырех крупных инициативах:

• Создание Новой технологической коалиции (ETC);

• Запуск Международной инициативы по цифровой демократии (IDDI);

• Осуществление скоординированного национального плана США по поддержке международных усилий; и

• Укрепление позиций Соединенных Штатов как международного центра цифровых исследований.

Действия для президента:

• Непосредственная разработка Международной научно-технической стратегии (MCT) межведомственной целевой группой под руководством Белого дома.

Президент должен руководить разработкой СПИСКОВ специальной целевой группой.

Целевая группа по MCTC должна созываться Советом по конкурентоспособности технологий или иным образом возглавляться Помощником Президента по вопросам национальной безопасности и директорами Управления научно-технической политики и Национального экономического совета.

Целевая группа атеистов должна включать в себя руководство следующих ведомств:

Государственный департамент;

инистерство финансов;

Министерство торговли, включая Бюро промышленности и безопасности (BIS) и Национальный институт стандартов и технологий (NIST);

Министерство энергетики (DOE);

Агентство кибербезопасности и инфраструктурной безопасности Министерства внутренней безопасности (CISA);

Национальный научный фонд (NSF);

Агентство США по международному развитию (USAID);

Американская Международная финансовая корпорация развития (DFC);

Экспортно-импортный банк Соединенных Штатов (EXIM);

Агентство США по торговле и развитию (USTDA);

Корпорация «Вызов тысячелетия» (MCC); и

в соответствующих случаях-другие учреждения, обладающие опытом работы по отдельным темам.

Целевая группа по ИСБ должна разработать и представить Президенту официальную стратегию, тесно связанную со Стратегией национальной безопасности Президента (СНБ) и Совместным стратегическим планом госсекретаря и Администратора ЮСАИД (СП), опираясь на цели и приоритеты этих документов, связанные с технологиями. Атеисты должны служить международным компонентом Национальной технологической стратегии.

Необходимо быть сосредоточеным вокруг четырех крупных инициатив, рассматриваемых в этом плане:

создание новой технологической коалиции;

запуск Международной инициативы по цифровой демократии;

реализация всеобъемлющего национального плана США по поддержке международных цифровых усилий в области технических стандартов, иностранной помощи, финансирования развития и экспортного контроля; и

укрепление позиций Соединенных Штатов как международного центра цифровых исследований.

После утверждения Президентом Целевая группа по стратегии будет отвечать за надзор и поддержку осуществления, включая определение ресурсов и организационных изменений, необходимых для реализации стратегии. Целевая группа атеистов должна проводить регулярные совещания для содействия осуществлению стратегии.

Рекомендация: Создание новой технологической коалиции

В рамках ИСТ Соединенные Штаты во главе с Белым домом и Госдепартаментом должны возглавить формирование Формирующейся

Технологической коалиции (ИТП) стран, уважающих демократические ценности. ЭТП будет представлять собой орган единомышленников-союзников и партнеров, которые будут работать друг с другом и с помощью международных и неправительственных организаций, субъектов гражданского общества и частного сектора в целях разработки и осуществления скоординированной стратегии и связанной с ней политики в целях:

1. содействовать разработке, развитию и использованию новых технологий в соответствии с демократическими нормами и ценностями;

2. координация политики и инвестиций для противодействия пагубному использованию этих технологий авторитарными режимами; и

3. обеспечьте конкретные, конкурентоспособные альтернативы для противодействия внедрению цифровой инфраструктуры, созданной в Китае.

Действия для Белого дома и Государственного департамента:

• Созыв ключевых союзников и партнеров для присоединения и создания ИТД.

Соединенные Штаты должны возглавить ЭТП стран-единомышленников либо в рамках более крупного демократического саммита, либо в качестве самостоятельного начинания.

Членство должно включать в себя основную группу технологически развитых демократических стран, отражающих широкое географическое распределение, которые продемонстрировали общие интересы в продвижении ответственного ИИ, противодействии пагубному использованию новых технологий и обеспечении высоких стандартов открытости, доверия и конфиденциальности в цифровой инфраструктуре.

ИТЦ должен опираться на два важных диалога, ранее рекомендованных Комиссией: Американо-индийский стратегический технологический альянс и Стратегический диалог США-ЕС по новым технологиям.

ИТП должна опираться на перспективные усилия и проекты, осуществляемые Организацией экономического сотрудничества и развития (ОЭСР) и Глобальным партнерством по ИИ (ГПАИ), и дополнять их.

Ключевые многосторонние технологические инициативы (находятся в конце этого Плана).

Комиссия далее рекомендует ЭТП пригласить представителей международных организаций, неправительственных организаций, гражданского общества, научных кругов и частного сектора.

Эти организации имеют решающее значение для осуществления трансграничной политики, объединения государственных и негосударственных субъектов и содействия согласованию ответственного развития ИИ и цифровой инфраструктуры в соответствии с общими демократическими ценностями.5

Они должны быть включены в состав ЭТП, в число участников инаугурационной сессии и иметь статус наблюдателя.

Действия в интересах Соединенных Штатов, их союзников и партнеров:

• Организация усилий по синхронизации политики и инициатив в семи важнейших областях.

ИТП должна быть организована вокруг конкретной повестки дня с практическими целями, ориентированными на результаты, а не на процессы, предназначенными для разработки и реализации общего видения позитивного технологического будущего и противопоставления его будущему, в котором доминируют авторитарные практики.

Опираясь на существующую систему руководящих принципов, таких как Принципы ИИ ОЭСР,6 члены должны использовать первое совещание для утверждения конкретной повестки дня, предназначенной для практической реализации политики и инициатив в семи важнейших областях:

Разработка и внедрение стандартов и норм в поддержку демократических ценностей и развитие безопасных, надежных и надежных технологий;

Содействие и содействие скоординированным и совместным НИОКР в области искусственного интеллекта и цифровой инфраструктуры, которые продвигают общие интересы и приносят пользу человечеству;

Содействие демократии, правам человека и верховенству закона посредством совместных усилий по противодействию цензуре, вредоносным

информационным операциям, торговле людьми и нелиберальному использованию технологий слежки;

Изучение путей облегчения обмена данными между союзниками и партнерами с помощью благоприятных соглашений, общих процедур архивирования данных, совместных инвестиций в технологии повышения конфиденциальности и устранения правовых и нормативных барьеров;

Поощрение и защита инноваций, в частности посредством экспортного контроля, скрининга инвестиций, обеспечения цепочек поставок, инвестиций в новые технологии, торговой политики, исследований и киберзащиты, а также согласования интеллектуальной собственности;

Развитие талантов, связанных с искусственным интеллектом, путем анализа проблем рынка труда, гармонизации требований к навыкам и сертификации, а также расширения обмена талантами, совместного обучения и инициатив по развитию рабочей силы;

Запуск Международной инициативы по цифровой демократии для координации международной внешней помощи, помощи в целях развития и финансирования, технического руководства и политического руководства.

Чтобы выполнить повестку дня по семи критическим областям, члены ЕТС должны рассмотреть возможность создания групп реализации для каждой области.

Предлагаемые повестки дня и руководящие указания по каждой критической области включены в Приложение Коалиции за новые технологии к настоящему Плану действий.

Рекомендация: Запустить Международную инициативу цифровой демократии

Комиссия рекомендует Соединенным Штатам и государствам-партнерам ЕТС запустить Международную инициативу цифровой демократии (IDDI) - скоординированные усилия по согласованию политики и программ внешней помощи государств-партнеров для разработки, продвижения и финансирования внедрения ИИ и связанных с ним технологий, которые соответствуют

демократическим ценностям и этическим нормам открытости, конфиденциальности, безопасности и надежности.7 IDDI будет:

• Координация подходов государств-партнеров к внедрению и управлению цифровыми технологиями;

• Мобилизовать коалиционные усилия для предоставления альтернатив (через финансовую помощь, развитие технологий и инвестиции частного сектора) цифровой инфраструктуре и технологиям с поддержкой искусственного интеллекта/машинного языка (ИИ), которые используются в нелиберальных целях, а также для продвижения технологий, способствующих демократическому участию, правам человека и верховенству права; и

• Содействовать внедрению безопасной, надежной и надежной цифровой инфраструктуры, технологий с поддержкой искусственного интеллекта/мл и информационно-коммуникационных технологий (ИКТ).8

Действия в интересах Соединенных Штатов, их союзников и партнеров:

• Координировать национальные стратегии, которые ДОПОЛНИТЕЛЬНО формулируют вовлечение.

Соединенные Штаты и партнеры по ИДДИ должны предпринять шаги по координации разработки национальных стратегий участия ИДДИ. Сосредоточив внимание на разработке и инвестировании в демократически выровненные цифровые технологии и поддержке проектов цифрового развития, инфраструктуры и наращивания потенциала, национальные стратегии IDDI должны способствовать достижению всеобъемлющих целей ETC. На рисунке ниже представлен обзор IDDI.

Комиссия рекомендует партнерам по ИДДИ стремиться к согласованию национальных стратегий на основе общих руководящих принципов для инвестиционных стратегий, критических технологий, политического руководства и поощрения экспорта. План публичной дипломатии и связанные с ним ресурсы также должны занимать видное место в каждой национальной стратегии, учитывая важность продвижения позитивного, единого послания о преимуществах и важности ИДДИ.

Обзор стратегии IDDI.

• Провести оценку глобального ландшафта цифрового развития.

Государствам-партнерам ИДДИ следует созвать совещание с участием представителей агентств по развитию и международных финансовых учреждений (МФИ) для проведения оценки цифровых подключений и глобальной среды цифрового развития в целях руководства деятельностью ИДДИ.9

Комиссия предлагает, чтобы эта оценка включала:

Глобальная оценка рисков государственной политики, финансовых и инвестиционных инструментов, технологий наблюдения и других механизмов, подрывающих неприкосновенность частной жизни, гражданские права и права человека. Эта оценка послужит основой для определения приоритетов ИДДИ.

Идентификация технологий или технологических особенностей для продвижения в рамках деятельности IDDI, включающей некоторые или все из следующих:

• защита конфиденциальности, такая как сохранение конфиденциальности мл, eyes-off мл, расширенное шифрование и безопасные многопартийные вычислительные модели;

• защита от нежелательной предвзятости в данных и выводах;

• ограничения на использование определенных приложений для предотвращения потенциального нарушения гражданских и человеческих прав;

• ограничения на хранение данных и доступ к ним, чтобы предотвратить доступ третьих лиц, нескольких государственных учреждений и иностранных правительств;

• безопасные, надежные инструменты искусственного интеллекта и цифровая инфраструктура;

• инструменты и инфраструктура для поддержки «зеленых» инициатив, включая интеллектуальные сети; и

• инструменты для местного населения по противодействию авторитарному использованию ИИ в целях социального контроля.

Выявление передового опыта в рамках членов IDDI и существующих инициатив, которые обеспечивают прочную основу для развития и развития в масштабе. IDDI должен использовать уникальные возможности и ресурсы отдельных государств-партнеров IDDI.

Модели Международной инициативы по цифровой демократии

Следующие примеры усилий по разработке, продвижению и финансированию внедрения безопасных, надежных и открытых цифровых экосистем могут служить образцами для проектов IDDI.

Модели Международной инициативы цифровой демократии (IDDI).

Определение инвестиционных руководящих принципов для проектов технологического развития и цифрового развития и поддержка согласования через ОЭСР.

Инвестиционные решения в развитие конкретных технологий и финансирование различных проектов цифрового развития должны основываться на результатах оценки и согласованных принципах цифрового развития и использования ИИ. К ним относятся:

Принципы G20 для качественных инвестиций в инфраструктуру;

Принципы цифрового развития, используемые USAID для руководства усилиями по оказанию цифровой иностранной помощи

Критерии безопасности и доверия к Телекоммуникационным сетям и услугам, разработанные Государственным департаментом, Центром стратегических и международных исследований и внешними экспертами и используемые сетью Blue Dot;

Рекомендация ОЭСР по цифровой безопасности критически важных видов деятельности;

предстоящие Принципы ОЭСР о доверенном правительственном доступе к данным;

Руководящие принципы ОЭСР для многонациональных предприятий; и

Руководящие принципы ООН по предпринимательству и правам человека.

Члены IDDI также должны работать с ОЭСР над стандартизацией ИИ и помощью в области цифрового развития путем создания специального кода целей «Цифрового развития».

Специальный целевой код, контролируемый Комитетом содействия развитию ОЭСР (КСР), продемонстрирует международную решимость, облегчит координацию, позволит ОЭСР и другим структурам контролировать финансирование деятельности в области цифрового развития и консолидировать данные для принятия стратегических решений IDDI.

• Разработать руководящие принципы использования технологий в рамках IDDI.

Оценка рисков должна привести к разработке руководящих принципов использования приложений с поддержкой ИИ/мл и технологий эпиднадзора.

Эти усилия должны основываться на нескольких основополагающих документах, включая Принципы ИИ ОЭСР, а также Ключевые соображения NSCAI по ответственному развитию и внедрению искусственного интеллекта,19 которые обеспечивают оперативное руководство по ответственному и этичному развитию и использованию ИИ в инженерных практиках, производительности систем, взаимодействию человека и ИИ, а также подотчетности и управлению.

• Разработать принципы стимулирования экспорта и контроля за ним и координировать их принятие каждым государством-партнером.

Страны IDDI должны установить приоритеты для поощрения экспорта и научно-исследовательской деятельности в целях продвижения технологий, которые соответствуют общим демократическим ценностям и поддерживают свободные и открытые общества. Эти приоритеты могут быть расширены руководящими принципами ОЭСР и новыми руководящими принципами Государственного департамента США по надзору за должной осмотрительностью (см. Ниже о продвижении демократии через экспортный контроль), чтобы стимулировать компании против сделок, которые могут

привести к злоупотреблению технологиями государственными конечными пользователями.

• Расширение инвестиций государственного и частного секторов путем изучения вопроса о создании совместного инвестиционного фонда и стимулов для частных инвестиций.

Члены IDDI должны рассмотреть возможность создания совместного инвестиционного фонда—с выделенным инвестиционным менеджером—для поддержки проектов IDDI. Такой фонд можно было бы смоделировать по образцу Инвестиционного фонда Инициативы трех морей (SIIF).

Поскольку инвестиции государственного сектора вряд ли достигнут масштабов, необходимых для реализации целей ИДДИ и обеспечения коллективной безопасности государств-партнеров ИДДИ, партнеры ИДДИ должны стремиться катализировать по меньшей мере 20 миллиардов долларов инвестиций частного сектора.

Члены IDDI могли бы изучить стимулы для инвестиций частного сектора в критически важные новые технологии, особенно в Индо-Тихоокеанском регионе, Латинской Америке и других регионах с высоким потенциалом роста. Политика, которую необходимо изучить, включает налоговые стимулы и субсидии, информирование частного сектора о приоритетах IDDI, привлечение внимания к инвестициям и практике частного сектора, способствующим достижению целей IDDI, а также повышение налогов на прибыль, получаемую от публично торгуемых компаний стратегических конкурентов.

• Проведение скоординированной стратегической кампании обмена сообщениями и повышения осведомленности.

Успех IDDI будет зависеть не только от скоординированной инвестиционной деятельности и помощи, но и от способности членов IDDI эффективно и стратегически донести цели до мировых лидеров, международных организаций и общественности.

Рекомендация: Разработать и реализовать Комплексный Национальный план США по поддержке международных технологических усилий.

Теисты должны включать в себя комплексный общегосударственный план координации инструментов внешней политики США для продвижения ETC, IDDI и автономных проектов. Этот план должен использовать технический опыт, иностранную помощь, финансирование развития и инвестиции, политическое руководство и экспортный контроль в поддержку трех основных целей:

1. Формирование международных технических стандартов в области искусственного интеллекта и связанных с ним технологий;

2. Осуществление скоординированной политики США в отношении IDDI;

3. Содействие прозрачности и подотчетности посредством экспортного контроля.

Диалог правительства США с американской промышленностью, а также демократическими союзниками может помочь преодолеть информационную асимметрию и прояснить цели технических стандартов на ИИ, которые способствуют экономическому росту, защите потребителей и защите демократических ценностей. Партнерство и обмен информацией между правительством США, промышленностью и научными кругами имеют решающее значение для обеспечения защиты интересов национальной безопасности, связанных со стандартами, и нейтральности международных органов, устанавливающих стандарты.

Действия для президента:

• Издать Исполнительный приказ в поддержку международной технической стандартизации.

Как подробно описано в Промежуточном отчете NSCAI и Рекомендациях за третий квартал, Президент должен издать исполнительный указ:

создать межведомственную координационную целевую группу для обмена информацией об угрозах и определения интересов национальной безопасности США, связанных с техническими стандартами искусственного интеллекта и связанными с ними стандартами, такими как международные стандарты науки о данных, возглавляемую NIST с участием представителей

Государственных департаментов, обороны, энергетики, торговли и национальной безопасности, Канцелярии директора национальной разведки и USAID;

поручить межведомственной целевой группе улучшить партнерство и сотрудничество с промышленностью и научными кругами;

поручить межведомственной целевой группе провести консультации с соответствующими комитетами Конгресса и разработать план работы с уполномоченными Конгресса по необходимым ресурсам и эквивалентам полного рабочего дня, необходимым для поддержки лидерства США в международной технической стандартизации;

направлять федеральные агентства на финансирование и поддержку целенаправленных исследований, испытаний и оценки, а также на регулярное и активное участие правительства США в деятельности по установлению международных стандартов;

требовать от директора NIST и Координатора по стандартам поощрения частного сектора к созданию Центра стандартизации для улучшения обмена передовым опытом и другой информацией, имеющей отношение к разработке стандартов, а также поддержки целенаправленной координации исследований;

создать федеральный консультативный комитет с участием экспертов из частного сектора и научных кругов для обеспечения стратегического руководства межведомственной координационной целевой группой по международным техническим стандартам.

Меры для Министерства торговли:

• Координация деятельности по разработке технических стандартов в масштабах всего правительства через руководство НИСТ межведомственной целевой группой.

Разработка международных стандартов для ИИ и новых технологий должна быть включена в общие МСТ. В правительстве США этот процесс должен по-прежнему возглавляться NIST при активном участии агентств в координационной целевой группе, описанной выше.

Комиссия предложила всеобъемлющий план для NIST и других департаментов и агентств США, чтобы обеспечить, чтобы разработке международных технических стандартов уделялось больше внимания и ресурсов для обеспечения того, чтобы интересы национальной безопасности США, включая продвижение технологий, согласующихся с демократическими ценностями, продвигались в организациях по разработке стандартов.

НИСТ и другие учреждения должны учитывать Ключевые соображения Комиссии по ответственной разработке и внедрению ИИ при оценке позиций по техническим стандартам.

• Созвать федеральный консультативный комитет для информирования стратегии о международных стандартах.

Как отмечалось выше, в предлагаемом Исполнительном указе будет создан федеральный консультативный комитет для предоставления межведомственной целевой группе экспертных рекомендаций по информированию правительства США о стратегии в области международных технических стандартов.

лены консультативного комитета должны быть привлечены из частного сектора и научных кругов и должны быть отобраны межведомственной целевой группой за их опыт в новых технологиях, геополитическом анализе, глобальных экономических тенденциях и аналогичных областях.

Комиссия предполагает, что этот консультативный комитет, сосредоточившись на стратегических геополитических вопросах вокруг международных технических стандартов, будет выполнять функцию, которую в настоящее время не выполняют другие консультативные группы и отраслевые организации, координирующие позиции США в международных органах по стандартизации.

Консультативный комитет должен иметь перспективный мандат на участие в стратегии правительства США по целому ряду новых технологий, включая технологии, связанные с геномикой, цифровой валютой, производством биофармы и другими.

NIST и Госдепартамент должны обеспечить, чтобы члены получили соответствующие разрешения для облегчения обмена секретной информацией, необходимой для разработки стратегии США.

Меры для Министерства торговли и государственного управления:

• NIST при содействии Государственного департамента должен координировать деятельность по разработке технических стандартов на международном уровне.

Кроме того, NIST, работая в тесном сотрудничестве с Государственным департаментом—в идеале, в контексте ETC и IDDI—должен уделять приоритетное внимание взаимодействию с демократическими странами для согласования позиций по стандартам, имеющим решающее значение для взаимной безопасности и обороны, и обеспечивать, чтобы эти позиции отражались в обсуждениях организаций по разработке технических стандартов.

Региональные технические сотрудники Госдепартамента могут служить проводниками для этого выравнивания (см. ниже «Переориентация внешней политики США и Госдепартамента»).

Действия для Конгресса:

• Обеспечить надлежащее финансирование NIST и других департаментов и агентств США для поддержки международных усилий по технической стандартизации.

Как рекомендовала Комиссия, Конгресс должен предоставить средства, достаточные для поддержки по крайней мере шести штатных сотрудников в NIST и по крайней мере одного штатного сотрудника в Государственном департаменте, Министерстве обороны, Национальной безопасности и энергетике, Канцелярии директора национальной разведки, USAID и других соответствующих учреждениях. Эти сотрудники будут поддерживать координатора по стандартам ИИ NIST, поддерживать целенаправленные исследования и

выполнять другие обязанности, необходимые для технической стандартизации, такие как участие в организациях по разработке стандартов.

• Обеспечить надлежащее финансирование и выдачу грантов Государственному департаменту для обеспечения международного лидерства в разработке технических стандартов.

Как рекомендовала Комиссия, Государственный департамент должен иметь надлежащие ресурсы для полноценного участия в международных форумах, профсоюзах и организациях, занимающихся разработкой стандартов для ИИ, связанных с ними технологий и данных. Конгресс должен выделить минимум 5 миллионов долларов на поддержку этих усилий, в частности на привлечение и финансирование американских ученых и исследователей для участия в этих международных форумах. Это действие может потребовать создания нового фонда иностранной помощи и органа по выдаче грантов Департаменту.

• Создать грантовую программу, позволяющую малым и средним американским компаниям ИИ участвовать в международных усилиях по стандартизации.

Как рекомендовала Комиссия, Конгресс должен разрешить грантовую программу для малых и средних американских компаний ИИ, чтобы покрыть высокие затраты на участие в международных усилиях по стандартизации, включая проведение соответствующих исследований, развитие необходимых навыков и опыта, подготовку предложений по стандартам и участие в технических совещаниях по установлению стандартов. Их вклад способствует расширению технологических инноваций, помогает предотвратить потенциальные высокие «затраты на переключение», которые могут препятствовать их росту, и облегчает разработку решений для стандартов, препятствующих экспорту этих малых предприятий.

Комиссия предлагает Конгрессу выделять первоначальную сумму в размере 1 миллиона долларов ежегодно для финансирования грантов, выдаваемых Администрацией малого бизнеса в координации с NIST.

Компонент 2: Осуществление скоординированной национальной политики США в отношении IDDI

Национальная политика в отношении усилий США в области цифрового развития и участия в IDDI обеспечит стратегическое видение высокого уровня и координацию, необходимые для:

• Продвигать интересы Соединенных Штатов и их союзников и партнеров в разработке и глобальном внедрении технологий с поддержкой ИИ/мл и безопасных, надежных и открытых цифровых экосистем, которые продвигают ценности, критически важные для свободного и открытого общества;

• Повысить во всех департаментах и ведомствах США приоритетность цифрового развития, необходимого для продвижения интересов США и целей IDDI, а также переориентировать усилия США в области развития на цифровую эпоху;

• Укрепление внешней политики США за счет значительных ассигнований на цифровое развитие, увеличения ресурсов и кадрового обеспечения, а также расширения полномочий федеральных ведомств и агентств, в частности Государственного департамента, USAID и DFC.

Действия для Целевой группы ISTS:

• Разработать в рамках ИГИЛ национальную стратегию США по продвижению цифровых технологий и поддержке цифрового развития, инфраструктуры и наращивания потенциала.

Они должны включать комплексный и комплексный подход к инструментам внешней помощи и финансирования развития правительства США. Это позволит скоординировать участие США в более широких усилиях IDDI и обеспечит дорожную карту для более эффективного использования государственных ресурсов США для поддержки развития цифровой инфраструктуры и демократического внедрения ИИ и новых технологий.

В стратегии также должна быть подробно описана стратегическая информационно-пропагандистская кампания, направленная на разоблачение нарушений международных стандартов и демократических норм авторитарными государствами.

На приведенном ниже рисунке показаны основные заинтересованные стороны США и их предполагаемая роль в общегосударственных усилиях. Комиссия рекомендует разработать конкретные планы учреждений по осуществлению этой стратегии.

Национальный план США по поддержке международных технологических усилий.

NIST-это нерегулируемое агентство Министерства торговли, а BIS-это бюро в Министерстве торговли.

• Провести оценку существующих программ в правительстве США и связанных с ними финансовых, кадровых и властных структурах подразделений Целевой группы ISTS.

Целевая группа теистов должна провести раннюю оценку, чтобы направлять развитие этой части теистов. Оценка должна включать в себя:

Оценка текущих и недавних межведомственных программ для выявления передовой практики и приоритетных стран, а также рамок управления данными и многосторонних обязательств, на которых могут быть основаны более всеобъемлющие усилия.

Оценка полномочий, ассигнований и персонала, необходимых для достижения целей национальной стратегии.

Целевая группа THISTS также должна рассмотреть вопрос об удовлетворении неотложных потребностей в экспертах по новым технологическим вопросам с помощью инновационных программ ротации стипендий между государственным и частным секторами и внутригосударственных деталей.

Сотрудники CISA и Агентства перспективных оборонных исследовательских проектов (DARPA), например, могут помочь в решении неотложных задач в Государственном департаменте и USAID.

Действия для USAID:

• Уделять приоритетное внимание реализации Цифровой стратегии и поддерживать неотложные потребности в ресурсах и организации.

Цифровая стратегия USAID33 - это амбициозный и необходимый пятилетний план развития и гуманитарной помощи, ориентированный на продвижение безопасных, надежных и открытых цифровых экосистем и ответственное использование технологий искусственного интеллекта.

Реализация проекта запаздывает из-за недостаточного финансирования, недостаточного кадрового обеспечения и бюрократических проблем. В настоящее время Цифровая стратегия управляется Технологическим отделом в рамках Центра инноваций, технологий и исследований Бюро по вопросам демократии, развития и инноваций (DDI).

Комиссия рекомендует Администратору USAID продолжать усилия по преобразованию парадигмы развития путем внедрения цифрового фонда в портфели USAID. С этой целью Администратор должен определить приоритетность Цифровой стратегии, (1) выступая за выделение Конгрессом ассигнований на финансирование программ цифровой стратегии (см. Ниже), (2) увеличивая штат разработчиков экспертами в области искусственного интеллекта, 5G и связи, а также кибербезопасности, как в штаб-квартире, так и в миссиях передового развертывания, (3) преобразовывая Технологический отдел в официальный центр в рамках DDI и (4) уделяя приоритетное внимание включению технологий и цифровых технологий во все усилия по развитию.

Немедленное увеличение штата может быть достигнуто путем расширения существующих партнерских отношений с частным и некоммерческим секторами путем прямого найма сотрудников, программ стипендий для исследователей и получения подробной информации от других федеральных агентств.

Долгосрочные кадровые потребности выиграют от создания поддержки иностранной службы из рекомендованного Центра, ориентированного на цифровую экспертизу, чтобы укрепить способность USAID выявлять потребности, оценивать риски и осуществлять программную деятельность в области цифрового развития.

Действие для DFC:

• Расширение официальных отношений с международными партнерами и частными фондами для расширения масштабов инвестиций DFC и проектов подключения через смешанные механизмы финансирования.

Дорожная карта воздействия DFC-это пятилетняя попытка катализировать 75 миллиардов долларов 25 миллиардов долларов от DFC, 50 миллиардов долларов от частного сектора и предоставить техническую экспертизу и поддержку для оптимизации воздействия на развитие. Дорожная карта воздействия предлагает «поднять инновации и технологии по крайней мере на 50% портфеля DFC» и выделить 5 миллиардов долларов на проекты цифровой инфраструктуры и расширение доступа в Интернет.

Нынешние власти ограничивают возможности DFC инвестировать в сделки с более высоким риском, что создает проблемы для масштабирования проектов цифровой инфраструктуры, особенно в развивающихся странах.

Инвестиции DFC оцениваются в соответствии с Федеральным законом о кредитной реформе, и DFC имеет ограниченные бюджетные полномочия на субсидирование долевого финансирования (150 миллионов долларов) и долгового финансирования и технической помощи (30 миллионов долларов).

DFC не может предоставлять льготное кредитование, в отличие от Китая и аналогичных агентств, таких как Японский банк международного сотрудничества и Европейский инвестиционный банк, а также Всемирный банк.

DFC должна углубить свои отношения с существующими и новыми международными партнерами, чтобы расширить сферу своего финансирования и инвестиций в акционерный капитал в пространстве цифрового развития.

Аналогичным образом, DFC должна расширять партнерские отношения с более широким кругом неправительственных организаций, чтобы использовать свои собственные ассигнования через смешанные механизмы финансирования, которые позволяют осуществлять инвестиции с более высоким риском.

Это может включать создание фонда цифровых технологий, который инвестирует в развитие безопасной, надежной цифровой инфраструктуры, технологий с поддержкой ИИ/мл и ИКТ с техническими функциями, которые соответствуют демократическим ценностям и этическим нормам открытости, конфиденциальности, безопасности и надежности.

Действия для Конгресса:

• Создать выделенный Фонд развивающихся технологий для зарубежных операций и связанных с ними программ USAID и Государственного департамента.

Недостаточное финансирование программ цифровой внешней помощи и финансирования США усугубляется конкуренцией с другими приоритетами финансирования и отсутствием гибкого распределяемого бюджета.

Конгресс должен санкционировать выделенный бюджетный счет, Фонд развивающихся технологий, для содействия целостному планированию цифровой иностранной помощи, проектов цифрового развития, программ новых технологий и других видов деятельности в рамках МСТ.

Комиссия предлагает, чтобы выделенный счет включал запросы на дополнительные целевые ассигнования для USAID и Государственного департамента.

Существующие программы, связанные с цифровыми технологиями, также могут быть объединены в Фонд развивающихся технологий.

• Выделять 200 миллионов долларов ежегодно на реализацию Цифровой стратегии USAID.

Комиссия рекомендует Конгрессу ежегодно выделять не менее 200 миллионов долларов на поддержку реализации Цифровой стратегии USAID Технологическим отделом в рамках DDI, при этом требуемое финансирование, вероятно, будет многократно выше. Эти фонды должны поддерживать программную деятельность, а также важнейшие потребности в найме персонала.

Эта сумма основана на запросе USAID на 2021 финансовый год в размере 82 миллионов долларов, который включает поддержку Фонда цифровой экосистемы, увеличение штата и программную деятельность.

• Выделять 300 миллионов долларов ежегодно на программы Государственного департамента в области новых технологий.

Комиссия рекомендует Конгрессу ежегодно выделять не менее 300 миллионов долларов на поддержку новых технологических программ и административных потребностей Государственного департамента, а также на создание небольшой межведомственной группы должностных лиц, обладающих опытом в новых технологических вопросах.

Эти средства должны включать в себя немедленную просьбу о дополнительных ассигнованиях, описанных далее в этом Плане действий, на 70 миллионов долларов для решения неотложных дипломатических усилий, программ и иностранных операций в области ИИ, новых технологий и данных.

Дополнительное финансирование будет поддерживать деятельность по оказанию иностранной помощи в области новых технологий и цифровой инфраструктуры, включая планирование, оценку и предоставление помощи. Фонды будут поддерживать целевые цифровые программы в нескольких областях, включая программы Государственного департамента, связанные с верховенством права (INL), демократией и правами человека (DRL), сотрудничеством в области безопасности (AVC, PM, ISN) и технической помощью (EB, STAS и другие).

• Обеспечить ДФК достаточными ассигнованиями для укрепления финансирования развития как инструмента достижения национальных целей.

Чтобы повысить способность правительства США использовать инструменты финансирования развития и инвестиций в акционерный капитал для дальнейшего выполнения миссии ISTS, Конгресс должен предоставить DFC 1 миллиард долларов гибкого программного финансирования для поддержки проектов цифрового развития.

• Повышение потенциала DFC в области смешанного финансирования развития на основе межведомственных партнерств.

Конгресс ограничил ассигнования, выделяемые USAID, MCC и Госдепартаменту на партнерство с DFC в смешанных сделках. USAID и Госдепартамент ограничиваются перечислением 50 миллионов долларов в целом распределенных по всем проектам, не ограничиваясь цифровыми.

По мере того как роль DFC в инвестициях в цифровое развитие будет возрастать, потребность в средствах Государственного департамента, USAID и MCC также возрастет, что потребует эквивалентного увеличения финансирования для поддержки усилий USAID, State и MCC digital и AIrelated, которые могут быть представлены для перевода средств в DFC.

Комиссия предлагает Конгрессу выделить в общей сложности 200 миллионов долларов Государственному департаменту, USAID и MCC для использования в инвестиционных программах DFC.

• Соответствующие средства для поддержки критических потребностей персонала в DFC.

Конгресс должен выделить средства, достаточные для того, чтобы DFC увеличила свой передовой развернутый персонал, расположенный в регионах, в которые DFC инвестирует.

В настоящее время 98% сотрудников DFC базируются в Вашингтоне, округ Колумбия, и эта должность находится в невыгодном положении по сравнению с иностранными финансовыми институтами развития (DFIS). Для сравнения, по оценкам DFC, одноранговые DFI имеют примерно в четыре раза больше сотрудников и базируются преимущественно в странах с низким и ниже среднего уровнем дохода.

Содействие прозрачности и подотчетности посредством экспортного контроля

Достижению целей ИСТ будет способствовать способность правительства США использовать мощь частного сектора США. Важнейшим

инструментом достижения этой цели является стимулирование экспорта технологий, соответствующих демократическим ценностям.

Меры для Министерства торговли и государственного управления:

• Разработка политики лицензирования конечных пользователей и экспортного контроля в рамках МСТ.

Министерство торговли через БМР должно использовать целевые меры контроля за конечным использованием и требования к отчетности о должной осмотрительности в области прав человека, чтобы предотвратить и удержать американские фирмы от предоставления проблемных государственных конечных видов использования ИИ и связанных с ними технологий.

БМР следует опираться на свой запрос 2020 года о публичных комментариях относительно путей усиления контроля и мониторинга передовых систем наблюдения—эта область может быть изучена для предотвращения использования вычислительных технологий для нарушений прав человека при одновременном содействии продвижению технологий, ориентированных на демократию. Правила, изданные в октябре 2020 года, предоставляют БМР право по своему усмотрению отказывать в выдаче экспортных лицензий на продукцию, которая может быть использована для нарушения или злоупотребления правами человека.

Эти более строгие правила экспортного контроля, координируемые с Целевой группой ISTS, могут способствовать этическому и ответственному использованию ИИ среди американских фирм, устанавливать стандарты для мировой промышленности и противодействовать нарушениям прав человека и гражданских прав.

Государственный департамент через Бюро по вопросам демократии, прав человека и труда (DRL), Международной безопасности и нераспространения (ISN) и военно-политическим вопросам (PM) должен расширить свои недавно выпущенные рамки для руководства бизнесом в оценке рисков нарушений прав человека при экспорте оборудования для наблюдения, одновременно укрепляя продвижение демократических ценностей.

В координации с Министерством торговли Государственный департамент должен расширить сбор данных и анализ нарушений прав человека, связанных с новыми технологиями и авторитарной цифровой практикой.

Рекомендация: Укрепить позиции Соединенных Штатов как Международного центра исследований новых технологий

Третий компонент программы-усиление роли Соединенных Штатов как международного научно-исследовательского центра новых технологий. Эти цели заключаются в том, чтобы:

• Содействие вкладу правительства США в совместные инициативы и технические стандарты, такие как Глобальное партнерство по ИИ (GPAI) и цифровые проекты ОЭСР;

• Укрепление талантов Соединенных Штатов, союзников и партнеров путем инвестирования в людей через программы развития рабочей силы, наставничества и обмена, осуществляемые при содействии рекомендованного Многостороннего исследовательского института ИИ (MAIRI);

• Развивать совместные исследовательские отношения и объединять исследовательские ресурсы для разработки технологий (особенно в гражданских приложениях), которые соответствуют демократическим ценностям и устраняют пробелы в коммерческих НИОКР, включая совместные исследования в области технологий, повышающих конфиденциальность; и

Дать возможность США и союзникам преодолеть текущие проблемы регулирования, препятствующие сотрудничеству, особенно в Европе, такие как ограничения на обмен данными и соглашения об ответственности.

Компоненты Международного центра цифровых исследований.

Компонент № 1: Поддержка международных цифровых и искусственных исследований и разработок

Международные усилия, такие как ГПАИ и инициативы ОЭСР в области искусственного интеллекта и цифровых технологий, являются важнейшими форумами для содействия согласованию усилий стран-единомышленников по продвижению ответственного и ориентированного на человека развития и

использования искусственного интеллекта. Исследования, проводимые Национальными научно—исследовательскими институтами ИИ, управляемыми NSF и другими агентствами США, а также другими программами федеральных департаментов и агентств, являются невероятным ресурсом, который должен поддерживать эти ключевые международные усилия и продвигать ИИ и цифровые цели США и их единомышленников.

Действия для Государственного департамента, OSTP и NSF:

• Формализовать отношения «центра экспертизы» с Глобальным партнерством по искусственному интеллекту (GPAI).

NSF должна оценить кандидатов на должность американского экспертного центра для GPA I. NSF должна представить рекомендацию директору OSTP для руководства переговорами с GPA.

NSF следует рассмотреть кандидатуры из числа своих лауреатов, связанных с ИИ, включая Национальные исследовательские институты ИИ или создав координационный центр всех институтов. NSF также должна предложить методы привлечения других научно-исследовательских агентств США, таких как Министерство энергетики и NIST, для поддержки центра экспертизы.

В координации с Государственным департаментом и OSTP NSF должна провести переговоры о меморандуме о взаимопонимании между NSF и GPAI для формализации поддержки центром рабочих групп GPAI.55

• Увеличить поддержку усилий ОЭСР в области искусственного интеллекта и цифровых технологий.

Правительство США должно расширить свое сотрудничество с инициативами ОЭСР в области искусственного интеллекта, включая инициативы Директората по науке, технологиям и инновациям и Обсерватории по политике в области искусственного интеллекта.56 Комиссия предлагает расширить отношения тремя способами:

Во-первых, NSF следует изучить методы поддержки программы ОЭСР «Переход на цифровые технологии»57 для содействия обмену данными между странами-партнерами.

Входные данные должны включать пилотные проекты по измерению трансграничных потоков данных, таксономии для сравнения инициатив стран в области данных или политики управления данными.

Во-вторых, Государственный департамент, OSTP и NSF должны искать возможности для согласования с союзниками и партнерами через руководящие принципы ОЭСР по данным, в частности путем продвижения основанных на ценности передовых практик сбора (например, с согласия и контроля со стороны доноров), документирования (например, для поддержки ответственного использования и качества), использования данных в НИОКР (например, с прозрачностью), а затем предоставления данных, используемых в опубликованных исследованиях, более широкому исследовательскому сообществу (например, для воспроизводимости).

В-третьих, ОСТП должна работать с ОЭСР над формализацией «сети исследовательских узлов» для координации усилий в области искусственного интеллекта и цифровых технологий, а также научно-исследовательских центров по всему миру. Политикам и исследователям будет очень полезна глобальная информационная платформа, которая позволит легче понять различные инициативы в области искусственного интеллекта и связанные с ними инициативы, а также текущие исследовательские усилия.

Действия для Конгресса:

• Обеспечить административное финансирование для поддержки научно-исследовательских вкладов США в ГПАИ.

Центры экспертизы, поддерживающие ГПД I, также оказывают административную и секретариатскую помощь (например, планирование пленарных заседаний ГПД). Поэтому Конгресс должен предоставить дополнительные ресурсы NSF для поддержки развития центра, административного персонала и ресурсов для использования исследований из

портфеля ИИ NSF, включая Национальные исследовательские институты ИИ, а также из других департаментов и агентств США по мере необходимости.

Комиссия рекомендует выделить минимум 3 миллиона долларов в течение трехлетнего периода.

Компонент № 2: Создание Многостороннего научно-исследовательского института искусственного интеллекта (MAIRI)

Многосторонний научно-исследовательский институт ИИ (MAIRI) обеспечит модель справедливых многосторонних исследований, облегчит НИОКР в области ИИ, основанные на сильных сторонах стран-единомышленников, и разработает глобальную рабочую силу ИИ следующего поколения. Имея физический центр, расположенный в Соединенных Штатах с виртуальным присутствием, MAIRI позволит проводить совместные исследования среди ключевых союзников и партнеров и вносить вклад в более широкие усилия отраженные в Формирующейся технологической коалиции и IDDI по сохранению свободных и открытых обществ, победе в глобальной технологической конкуренции и стимулированию инноваций в области искусственного интеллекта таким образом, чтобы они соответствовали демократическим ценностям. В конечном счете, для достижения этих целей MAIRI должна стремиться содействовать созданию федеративной сети исследовательских институтов по всему миру, а также национальных лабораторий и университетских центров.

Действия для NSF:

• Создание MAIRI в США и поддержка участия американских исследователей в MAIRI.

NSF должен создать MAIRI по образцу Международной исследовательской станции Банфа.58 У MAIRI должен быть физический центр в Соединенных Штатах, а также виртуальное присутствие. NSF должен предоставить MAIRI весь персонал, необходимый для обеспечения ее успеха.

Хотя NSF не требует дополнительных полномочий для создания MAIRI, законодательство может облегчить этот процесс (см. раздел действия для Конгресса).

MAIRI должна быть разработана с достаточной гибкостью, чтобы обеспечить участие исследователей из промышленности, академических кругов, исследовательских институтов и благотворительных организаций на проектной основе; другие департаменты и агентства США, такие как Министерство энергетики, могут иметь решающее значение для использования всей экосистемы НИОКР США.

Программы NSF через Управление международной науки и техники (OISE) могут поддержать MAIRI, содействуя привлечению американских исследователей.

AccelNet59 может финансировать поездки, виртуальные сети и другие мероприятия, необходимые для поддержки исследовательских проектов между исследовательскими сетями.

МУЛЬТИПЛИКАТОР60 может поддерживать поездки предметных экспертов для определения возможностей сотрудничества с членами-учредителями или со странами, которые рассматривают возможность присоединения к MAIRI.

• Определить ключевых союзников и партнеров, которые станут членами-основателями MAIRI.

NSF, в тесной координации с Государственным департаментом, должен определить и обсудить участие членов-учредителей.

Комиссия рекомендует, чтобы членами-учредителями были Австралия, Канада, Франция, Германия, Италия, Япония, Новая Зеландия, Южная Корея и Соединенное Королевство.

Эти страны имеют существующие соглашения и отношения сотрудничества с Соединенными Штатами, которые можно было бы с большей готовностью использовать для развития центра. Они также обладают

обширными исследовательскими возможностями и разделяют ценности и интересы с Соединенными Штатами.

Приоритетным должно быть расширение за счет включения дополнительных союзников и партнеров; например:

Участие Европейского союза должно быть приоритетом; однако включение ЕС в MAIRI будет зависеть от способности преодолеть разногласия между ЕС и Соединенными Штатами по вопросам регулирующего законодательства, ответственности, финансирования, обмена данными и интеллектуальной собственности.

Участие Индии также должно быть приоритетным по мере развития MAIRI, опираясь на рекомендованный Комиссией Американо-индийский стратегический технологический альянс.

• Разработка принципов целостности исследований совместно с членами-основателями MAIRI.

Члены-основатели согласятся с совместно определенными Принципами многосторонних исследований ИИ, которые будут основываться на важности целостности исследований. Принципы могут включать в себя необходимость прозрачности, особенно при раскрытии информации о финансировании и международных связях; необходимость открытых данных и обмена данными; разработку систем оценки рисков и выгод; и использование основанных на заслугах конкурсных обзоров исследовательских предложений.

Члены Совета также пройдут обучение по вопросам рисков безопасности и согласятся использовать надежную инфраструктуру в качестве части основополагающих принципов (см. рекомендуемые ассигнования в разделе «Действия для Конгресса»).

В соглашении также будут подробно изложены условия обращения с интеллектуальной собственностью, обмена данными, регулирующего законодательства и ответственности, а также финансирования.

• Разработать конкретную программу исследований с членами-основателями MAIRI.

Как только члены-основатели согласятся с Принципами, они определят основные направления и инициативы. Страны будут финансировать участие своих исследователей в совместных проектах. Совместные исследовательские проекты будут осуществляться через виртуальные пространства, а также в партнерских организациях, таких как исследовательские институты и университеты, которые получают финансирование от MAIRI. Могут также использоваться средства других участвующих департаментов и учреждений.61

Приоритеты исследований: Проекты должны быть выбраны таким образом, чтобы использовать сравнительные преимущества участников, позволяя участникам учиться у исследователей-партнеров. Примеры приоритетов в области НИОКР приводятся в Приложении Коалиции за новые технологии к настоящему Плану действий. Приоритеты должны включать:

Создание общих, безопасных вычислительных ресурсов (включая высокопроизводительные вычисления [HPC], облачные и квантовые вычисления), включая совместные проекты бенчмаркинга и инициативы по обмену данными, объединению и хранению данных, основанные на общепринятых принципах, обеспечивающих доверие, конфиденциальность и безопасность.

Технологии AI/мл, сохраняющие конфиденциальность, включая такие технологии, как федеративное обучение и прогнозирование на устройстве, которые позволяют удаленно выполнять зашифрованные вычисления с помощью многопартийных вычислений и гомоморфного шифрования, а также дифференциальную конфиденциальность.

Разработка технологий умных городов, согласованных с демократическими ценностями, которые способствуют устойчивому развитию, а также норм, которые должны направлять разработку стандартов в таких органах, как МСЭ и органы по техническим стандартам.

• Координировать с членами-основателями MAIRI вопросы финансирования, международных соглашений и структур управления.

Хотя Соединенные Штаты должны финансировать первоначальные затраты на запуск, включая приобретение физического центра MAIRI, персонала и виртуальной исследовательской/сетевой инфраструктуры (см. Рекомендации Конгрессу ниже), каждый член должен впоследствии предоставлять пропорциональные финансовые взносы на НИОКР MAIRI и участие своих исследователей в спонсируемых MAIRI семинарах и конференциях по образцу подхода, используемого Международной исследовательской станцией Банфа.64

Что касается текущих операций, то MAIRI следует изучить потенциал развития эндаумента по образцу трех американо-израильских бинациональных фондов. Такой подход облегчил бы использование благотворительных пожертвований для поддержки MAIRI.

Umbrella international AI/S&T agreements—переговоры с NSF, членами MAIRI и американскими агентствами—будут способствовать сотрудничеству между союзниками и партнерами за пределами MAIRI.

После создания MAIRI может поддерживать ГПД и другие международные усилия. MAIRI также следует заключить исследовательские соглашения с другими центрами передового опыта и исследовательскими центрами, ориентированными на AIR&D, чтобы создать федеративную сеть исследовательских институтов по всему миру.

Члены MAIRI также должны определить, как они будут определять расширение членства MAIRI, особенно в Европейском союзе и Индии.

Действия для других департаментов и агентств США:

• Поддержка создания MAIRI и ее НИОКР.

NSF будет американским якорным партнером для MAIRI. Его успех требует привлечения всей экосистемы исследований и разработок США и государственных исследовательских организаций.65 Важнейшими партнерами должны быть, в частности, Министерства энергетики и государства, а также NIST.

Министерство энергетики должно использовать свои национальные лаборатории, историю работы с промышленностью, огромные технические возможности, опыт прикладных исследований и опыт в области HPC и квантовых вычислений.

Государственный департамент должен обеспечить внешнеполитическую экспертизу и дипломатию, в том числе путем назначения специального сотрудника дипломатической службы для поддержки создания MAIRI, а также выявления полезных проектов.

Другие федеральные органы, включая Национальные институты здравоохранения, Национальное управление океанических и атмосферных исследований (НОАА) и Министерство здравоохранения и социальных служб, будут иметь решающее значение для технической экспертизы и сотрудничества в рамках целевых исследовательских проектов.

Действия для Конгресса:

• Принять закон, официально разрешающий MAIRI.

Хотя это и не требуется для создания MAIRI, Конгресс должен принять закон, формально разрешающий создание MAIRI и разъясняющий полномочия других исполнительных органов по предоставлению финансирования MAIRI. Это послужит сигналом о важности международного сотрудничества в области искусственного интеллекта и обеспечит наличие у НСФ и партнерских агентств достаточно надежных полномочий для достижения своих целей.

Законодательство должно также конкретно санкционировать и направлять NSF, в координации с Государственным департаментом, создание надежного обучающего облака и связанного с ним вычислительного потенциала для содействия международным совместным исследованиям.

Доверенное обучающее облако обеспечит доступ к необходимым ресурсам, вычислительным ресурсам и данным для совместных инноваций и разработки стандартов обмена данными, которые могли бы стать моделью для более широкой международной системы обмена данными.

• Поддержка создания MAIRI путем соответствующего финансирования NSF и других критически важных учреждений.

Комиссия рекомендует Конгрессу выделить минимум 60 750 000 долл. США на пятилетний период, который будет дополнен взносами международных партнеров.

Предлагаемые ассигнования распределяются следующим образом:

10 миллионов долларов в год в течение пяти лет NSF и другим критически важным агентствам (таким как Министерства энергетики и штата) для исследовательских инициатив.

2 миллиона долларов в год в течение пяти лет NSF для создания и поддержания физического центра, расположенного в Соединенных Штатах, связанной с ним инфраструктуры и административных операций.

150 000 долларов в год в течение пяти лет NSF для поддержки поездок американских исследователей и связанных с ними расходов на участие в семинарах, конференциях и других мероприятиях MAIRI в физическом центре.

Комиссия рекомендует Конгрессу выделять 11,25 миллиона долларов в год на исследовательские инициативы, направленные на создание надежного обучающего облака и связанных с ним вычислительных мощностей для содействия международным совместным исследованиям.

• Создать фонд для MAIRI для поддержки текущего финансирования.

MAIRI, возможно, пожелает создать эндаумент-фонд по аналогии с американо-израильскими бинациональными фондами. Если это будет продолжено, Конгресс должен санкционировать этот эндаумент-фонд и поддержать первоначальные инвестиции США. Потребуются дополнительные ассигнования для поддержки секретариата целевого фонда MAIRI.

Компонент № 3: Расширение обмена талантами

Соединенные Штаты должны привлекать талантливых людей к совместным исследованиям как в Национальных исследовательских институтах ИИ, так и в MAIRI. Устойчивое, прочное сотрудничество между партнерами MAIRI имеет решающее значение для обеспечения того, чтобы ответственный,

безопасный, ориентированный на человека ИИ преобладал над авторитарным ИИ. Исследования плечом к плечу и обмен талантами бесценны, позволяя исследователям строить отношения, учиться друг у друга, обмениваться идеями и стимулировать будущее сотрудничество.

Действия для Государственного департамента:

• Использовать визовые программы O и J для привлечения квалифицированных исследователей для поддержки программ MAIRI и международного обмена талантами.

Государственный департамент в координации с Министерством внутренней безопасности должен использовать визовые программы O и J для облегчения поездок иностранных исследователей в Соединенные Штаты для совместной работы с исследователями из Соединенных Штатов и других стран. Количество виз, выданных в рамках этих программ, не ограничено законом.

Рекомендация: Переориентировать внешнюю политику США и Госдепартамент на конкуренцию Великих держав в цифровую эпоху

В ближайшей перспективе крайне важно создать координационный центр Государственного департамента по вопросам новой технологической политики, экспертных знаний и ресурсов с помощью мер, предлагаемых Комиссией ниже. В долгосрочной перспективе Соединенные Штаты должны коренным образом реорганизовать структуру, направленность и культуру Государственного департамента, чтобы продвигать американские интересы на стыке демократии, технологий, безопасности, торговли и прав человека.68 Без поддержки высокого уровня в Министерстве технологическая конкуренция вряд ли станет ключевым аспектом внешней политики США.

Действия для президента:

• Распространить среди руководителей Миссий президентское письмо-инструкцию, в котором новые технологии рассматриваются как неотделимые от основных геополитических интересов США.

Эта инструкция должна предписывать каждому руководителю Миссии разработать новый технологический план в рамках своей стратегии миссии, представляемый государственному секретарю.

Действия для Государственного департамента:

• Государственный секретарь должен поручить заместителю Государственного секретаря по вопросам управления и ресурсов (D/MR) возглавить работу по переориентации и реорганизации Департамента технической дипломатии.

В прошлом должность D/MR осуществляла руководство по надзору за значительными организационными и ресурсными приоритетами в Государственном департаменте.

Бывшие чиновники на посту D/MR возглавляли дипломатические приоритеты США в области региональной политики (например, Стратегический диалог между США и Пакистаном), внешней помощи, гражданского реагирования и международных экономических вопросов.

D/MR должен обеспечить руководство в отношении немедленного и долгосрочного планирования для координации разрозненных офисов и бюро в рамках Государственного департамента, развития технологического опыта на всех уровнях Внешней и гражданской службы и обеспечения того, чтобы направление политики согласовывалось с действиями руководства, персонала и ресурсов, необходимыми для достижения переориентации с неотложностью и устойчивостью.

D/MR также должен обеспечивать руководство выполнением IST.

• Подготовить всеобъемлющее предложение о неотложных потребностях в финансировании с просьбой к Конгрессу о дополнительных ассигнованиях.

Госдепартамент должен подготовить и представить Конгрессу в течение 60 дней запрос о немедленном финансировании для решения проблемы нехватки кадров и программных усилий по дальнейшему развитию американской дипломатии вокруг новых технологий. Департаменту следует

изыскивать финансирование за счет дополнительных ассигнований, чтобы избежать задержек в бюджетном цикле.

• Ускорить создание специального бюро по дипломатии новых технологий.

Госдепартамент должен ускорить и расставить приоритеты в работе по кадрам, ресурсам и созданию бюро по дипломатии новых технологий.

Бюро безопасности киберпространства и новых технологий (CSET Bureau), официально утвержденное в январе 2021 года, призвано сосредоточиться на проблемах безопасности, связанных с киберпространством и новыми технологиями.70 Комиссия предлагает создать Бюро кредитных историй с широкими возможностями для решения дипломатических задач в области безопасности, экономики, прав человека и региональных аспектов внешней политики. Он должен служить координационным центром для оценки стратегических, бюджетных и кадровых приоритетов в отношении формирующейся технологической политики во всем Департаменте. Бюро должно нести ответственность за ведение диалога на высоком уровне с союзниками и партнерами в целях дальнейшего прогресса и сотрудничества, координацию политики, стандартов и помощи в цифровом развитии с американскими агентствами, а также содействие пропаганде ИИ и новых технологий в рамках Департамента.

Департаменту следует оценить, где следует разместить Бюро КСЭБ для наилучшего достижения этих целей, но при этом обеспечить, чтобы его создание не затягивалось еще больше.

Бюро должно возглавляться высокопоставленным помощником секретаря или послом по особым поручениям. Если Департамент назначает Помощника секретаря во главе Бюро и руководит координацией по всему Департаменту, ему следует рассмотреть вопрос о создании отдельной должности посла по особым поручениям для руководства дипломатией с иностранными коллегами по вопросам кибербезопасности и новых технологий.

• Разработать всеобъемлющий план реорганизации технологической дипломатии под руководством нового заместителя министра.

Государственному департаменту следует разработать всеобъемлющее предложение о создании должности заместителя министра по науке, исследованиям и технологиям (Q). State/Q объединит элементы для надежного, скоординированного подхода к научно—технической дипломатии в контексте конкуренции великих держав-с акцентом на новые технологии.71

State/Q также будет работать с директором по внешней помощи, чтобы управлять новым выделенным счетом для цифровой демократии и новых технологий и руководить внедрением IST во всем правительстве США.

В плане следует также рассмотреть вопрос о создании заместителей помощников секретарей по науке и технике в каждом региональном бюро. Эти должности обеспечивали бы важнейшую связь между техническими сотрудниками и высшим руководством.

В настоящее время в Департаменте отсутствует ядро старших, карьерных должностных лиц, обладающих глубоким и широким опытом в области технологической политики. Эти должности обеспечат карьерный рост сотрудников старшего звена, занимающихся вопросами технологической политики, и позволят руководителям высшего звена пропагандировать реформы, необходимые для эффективного управления технологической политикой.

Учитывая настоятельную необходимость укрепления потенциала Департамента в области технической дипломатии и вероятный долгосрочный характер процесса создания нового заместителя секретаря, усилия по осуществлению этой рекомендации должны осуществляться параллельно с другими организационными рекомендациями Комиссии.

• Установить дипломатическое присутствие в крупных технологических центрах США и других стран.

Госдепартамент должен усилить свое присутствие в крупных зарубежных и американских технологических центрах, опираясь на создание в миссиях

США кадрового состава специальных технических сотрудников для усиления дипломатической пропаганды, улучшения разведки технологий и информирования о политике и выборе иностранной помощи.

Департамент должен ускорить планы по созданию 12 региональных должностей технических сотрудников по всему миру и далее описать, как эти сотрудники повысят технологическую конкурентоспособность США с такими партнерами, как Иностранная коммерческая служба, USAID и DFC. Эти офицеры должны также разведывать технологические инициативы, которые могут укрепить наш дипломатический потенциал и потенциал развития.

Департамент должен восстановить постоянное присутствие в Кремниевой долине, которое он начал в 2014 году, и создать специальные должности в 2015-2016 годах. Эти должности и присутствие штата были прекращены, когда в январе 2017 года был введен мораторий на прием сотрудников ОМБ.

Кроме того, программа «Дипломат в резиденции» —с присутствием в 16 регионах в университетах по всей Америке73—должна быть перепрофилирована за рамки набора персонала и включать в себя публичную дипломатию, разведку технологий и взаимодействие с иностранными правительственными и коммерческими организациями, действующими по всей Америке. Внутреннее понимание является ценным вкладом во внешнюю политику и повысит доверие общественности к международному технологическому лидерству Америки и ее поддержку.

• Включить учебные модули по искусственному интеллекту и новым технологиям в курсы Института иностранной службы (FSI).

Государственный департамент должен включить обязательные модули, связанные с ИИ и новыми технологиями, в ключевые учебные курсы ФСИ, включая Посольский семинар, курсы заместителей начальников миссий, курсы политического и экономического ремесла и учебные курсы ориентации A-100. ФСИ также должна разработать отдельный курс по новым технологиям и внешней политике.

Департамент должен сотрудничать с академическими и частными организациями, чтобы получить доступ к передовым достижениям технологического образования, а также создать более надежную программу стипендиатов по технологиям для обмена с промышленностью.

Действия для Конгресса:

• Ускорить необходимую реорганизацию Государственного департамента путем принятия закона о создании заместителя министра по науке, исследованиям и технологиям (Q).

Конгресс должен действовать, чтобы создать позицию государства/Q и объединить разрозненные научно-технические усилия в Департаменте в одном подразделении. Существует настоятельная необходимость в такой реорганизации, и Конгресс может наделить Государственный департамент полномочиями, введя и приняв законодательство, чтобы ускорить переориентацию.

• Соответствующие средства для поддержки немедленного увеличения дипломатического корпуса США.

Конгресс должен обеспечить надежное финансирование для найма и обучения необходимого персонала, чтобы позволить Государственному департаменту переориентироваться и поддержать международные усилия Департамента по продвижению американских ценностей и стандартов в области ИИ, данных и связанных с ними новых технологий.

Комиссия рекомендует Конгрессу выделить дополнительные ассигнования в размере не менее 8 млн. долл.США для немедленного найма персонала для удовлетворения возникающих технологических потребностей во всех отделениях и бюро Департамента, установления дипломатического присутствия в крупных американских и зарубежных технологических центрах и разработки курсов FSI.

• Соответствующие средства для поддержки Бюро CSET.

Комиссия рекомендует выделить как минимум 20 млн. долл.

• Соответствующие средства для поддержки важнейших дипломатических усилий, программ и иностранных операций в области ИИ, новых технологий и данных.

Необходимо дальнейшее финансирование, чтобы Государственный департамент мог продвигать ответственный ИИ в соответствии с американскими ценностями и ценностями единомышленников.

Хотя подробная информация о потребностях в финансировании должна отражать вклад Государственного департамента, Комиссия рекомендует Конгрессу, как минимум, выделить дополнительные ассигнования на сумму не менее 37 млн. долл.:

Публичная дипломатия обмен сообщениями и вовлечение в поддержку демократических ценностей и повышение осведомленности о лидерстве США в области инноваций в области искусственного интеллекта а также о рисках нежелательной передачи технологий и авторитарных цифровых практик;

Программы обмена ИИ для продвижения ценностей США и финансирования участия развивающихся стран в многосторонней деятельности ИИ;

Программы для демонстрации американских инноваций и продвижения этического использования ИИ, включая программы American Spaces, TechCamp, MakerSpaces и US Speakers74;

Развитие партнерства и продвижение научных норм через программы научных посланников США и посольских научных стипендиатов;

Дипломатические операции и программы, связанные с международным сотрудничеством в области искусственного интеллекта, включая поддержку инициатив ИТП;

Поощрение прав человека и основных свобод в контексте ИИ;

Сохранение лидерства США в использовании ИИ в военных целях посредством сотрудничества с союзниками и партнерами;

Обеспечить политическую и политическую согласованность с союзниками и партнерами по использованию систем вооружения с поддержкой искусственного интеллекта;

Обеспечение постоянной оперативной совместимости между США и их союзниками и партнерами;

Подготовка кадров и наращивание потенциала иностранных правительств в области новых технологий для поддержки ответственных инноваций;

Отчетность по противодействию пагубному влиянию в экосистемах ИИ;

Расширение возможностей глобального научно-технического предпринимательства, ориентированного на искусственный интеллект, с помощью инициативы США Global Innovation through Science and Technology (GIST);

Инициативы общественной дипломатии по международным стандартам ИИ, а также отслеживание и отчетность об общественном мнении, связанном с ИИ.

Информационный бюллетень,

Государственный департамент США, Соединенные Штаты сотрудничают с Австралией и Японией в расширении Надежной и безопасной цифровой связи на Палау (29 октября 2020 года), https://2017-2021.state.gov/the-united-states-partners-with-australia-and-japan-to-expand-reliable-and-secure-digital-connectivity-in-palau//index.html; Информационный бюллетень, Государственный департамент США, 2020 Индо-Тихоокеанский бизнес-форум Продвигает свободный и открытый Индо-Тихоокеанский регион (29 октября 2020 года), https://2017-2021.state.gov/2020-indo-pacific-business-forum-promotes-free-and-open-indo-pacific/index.html; Запуск Многосторонней сети Blue Dot Network, Американской Международной финансовой корпорации развития (4 ноября 2019 года), https://www.dfc.gov/media/opic-press-releases/launch-multi-stakeholder-blue-dot-network; Blue Dot Network, Государственный департамент США (последний доступ 16 февраля 2021 года), https://www.state.gov/blue-dot-network/; Blue Dot Network: Frequently Asked Questions, Государственный

департамент США (последний доступ 16 февраля 2021 года), https://www.state.gov/blue-dot-network-frequently-asked-questions/; Digital Development Partnership (DDP), The World Bank (last accessed Feb. 16, 2021), https://www.worldbank.org/en/programs/digital-development-partnership; Годовой отчет Партнерства в области цифрового развития: Реагирование на кризис COVID-19, Всемирный банк (26 октября 2020 г.), https://www.worldbank.org/en/news/feature/2020/10/26/digital-development-partnership-annual-report-responding-to-the-covid-19-crisis; Цели, Инициатива трех морей (последний доступ 16 февраля 2021 года), https://3seas.eu/about/objectives; Three Seas Story, Three Seas Initiative (последний доступ 16 февраля 2021 года), https://3seas.eu/about/threeseasstory; Фонд Трех Морей Делает Свои Первые Цифровые Инвестиции, Инвестиционный Фонд Инициативы Трех Морей (2 Декабря 2020 Года), https://3siif.eu/news/the-three-seas-fund-makes-its-first-digital-investment; Фонд, Инвестиционный фонд Инициативы Трех морей (последний доступ 16 февраля 2021 года), https://3siif.eu/the-fund/; Пресс-релиз, США Международная финансовая корпорация развития, DFC Утверждает более 2,1 миллиарда долларов новых инвестиций в глобальное развитие (10 декабря 2020 года), https://www.dfc.gov/media/press-releases/dfc-approves-over-21-billion-new-investments-global-development; Пресс-релиз, Европейская комиссия, Западные Балканы: Экономический и инвестиционный план поддержки Экономического Восстановления и конвергенции(6 октября 2020 г.), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1811; Вопросы и ответы: Экономический и инвестиционный план для Западных Балкан, Европейская комиссия (6 октября 2020 г.), https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1819; Соединение Европы и Азии - Строительные блоки для Стратегии ЕС, Европейская комиссия (19 сентября 2018 г.), https://eeas.europa.eu/sites/eeas/files/joint_communication_-_connecting_europe_and_asia_-_building_blocks_for_an_eu_strategy_2018-09-19.pdf; Connecting Europe & Asia: The EU Strategy, European External Action

Service (Sept. 26, 2019), https://eeas.europa.eu/headquarters/headquarters-homepage/50699/node/50699_en; FAIR Forward - Искусственный интеллект для всех, Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH (июнь 2020 г.), https://toolkit-digitalisierung.de/app/uploads/2020/06/Factsheet-FAIR-Forward_E050620-1.pdf; Цели, открытые навсегда (последний доступ 16 февраля 2021 года), https://www.openforgood.info/; О проекте, проекте InDiCo (последний доступ к которому был получен 16 февраля 2021 года), https://www.indico-ictstandards.eu/about-the-project; Инициатива «Расширенное партнерство для качественной инфраструктуры», Направленная На Саммит G7 Ise-Shima, Объявленная Министерством экономики, торговли и промышленности Японии (23 мая 2020 года), https://www.meti.go.jp/english/press/2016/0523_01.html; Тобиас Харрис, ‘Качественная инфраструктура»: сильный вызов Японии Китайскому поясу и пути, Война на скалах (9 апреля 2020 г.), https://warontherocks.com/2019/04/quality-infrastructure-japans-robust-challenge-to-chinas-belt-and-road/; Андрея Бринза, Закон о балансе японского пояса и пути, Дипломат (нояб. 8, 2018), https://thediplomat.com/2018/11/japans-belt-and-road-balancing-act/; Программы Глобального сотрудничества и подготовки кадров (GCTF), Американский институт на Тайване (последний доступ 28 декабря 2020 года), https://www.ait.org.tw/our-relationship/global-cooperation-and-training-framework-programs-gctf/; Информационный бюллетень, Государственный департамент США, Поддержка США цифровых преобразований в Латинской Америке и Карибском бассейне (10 ноября 2020 г.), https://2017-2021.state.gov/u-s-support-for-digital-transformation-in-latin-america-and-the-caribbean//index.html.

Продвижение устойчивой инфраструктуры в Индо-Тихоокеанском регионе, USAID (последний доступ 16 февраля 2021 года), https://www.usaid.gov/sites/default/files/documents/1861/USAID_ITAN_Fact_Sheet_080719.pdf; Информационный бюллетень, Государственный департамент США, Партнерство умных городов США и АСЕАН (USASCEP): Обмен опытом между городами на благо народов АСЕАН (12 февраля 2021 года),

https://www.state.gov/u-s-asean-smart-cities-partnership-usascp-sharing-expertise-between-cities-to-benefit-the-people-of-asean/; Партнерство США-АСЕАН по умным городам, USASCP (последний доступ к февр. 16, 2021), https://www.usascp.org/home-page; Партнерство по цифровым связям и кибербезопасности (DCCP), USAID (19 октября 2020 г.), https://www.usaid.gov/digital-development/digital-connectivity-cybersecurity-partnership; Информационный бюллетень Посольства и Консульства США в Республике Корея, Индо-Тихоокеанский бизнес-форум 2020 года «Содействие свободному и открытому Индо-Тихоокеанскому региону» (29 октября 2020 года), https://kr.usembassy.gov/102920-2020-indo-pacific-business-forum-promotes-free-and-open-indo-pacific/; Пресс-релиз Посольства США в Чили, США Поддержка цифровой трансформации в Латинской Америке и Карибском бассейне (10 ноября 2020 года), https://cl.usembassy.gov/u-s-support-for-digital-transformation-in-latin-america-and-the-caribbean/; Информационный бюллетень, Государственный департамент США, Поддержка США цифровых преобразований в Латинской Америке и Карибском бассейне (10 ноября 2020 г.), https://2017-2021.state.gov/u-s-support-for-digital-transformation-in-latin-america-and-the-caribbean//index.html; USAID опубликовало такие ресурсы, как Отражение прошлого, Формирование будущего: Создание ИИ для международного развития и Управление проектами машинного обучения в международном развитии: Практическое руководство, отражающее Цифровую стратегию и излагающее демократические принципы внедрения этих технологий. См. Reflecting the Past, Shaping the Future: Making AI Work for International Development, USAID (21 мая 2019), https://www.usaid.gov/digital-development/machine-learning/AI-мл-in-development; Управление проектами машинного обучения в международном развитии: Практическое руководство, USAID (12 января 2021 г.), https://www.usaid.gov/digital-development/managing-machine-learning-projects; Цифровая стратегия 2020-2024, USAID, (июнь 2020 г.), https://www.usaid.gov/usaid-digital-strategy; Фонд цифровой экосистемы: Деятельность 2020 года, USAID (22 декабря 2020 года),

https://www.usaid.gov/digital-development/DEF2020; Дорожная карта воздействия, DFC (последний доступ 16 февраля 2021 года), https://www.dfc.gov/roadmap-for-impact; Информационный бюллетень, Экспортно-Импортный банк Соединенных Штатов, Обзор: Программа по Китаю и трансформационному экспорту (последний доступ 16 февраля 2021 года), https://www.exim.gov/who-we-serve/external-engagement/china-and-transformational-exports-program/fact-sheet#:~:text=EXIM%20is%20actively%20working%20to,or%20by%20other%20covered%20countries; Информационный бюллетень, Экспортно-Импортный банк Соединенных Штатов, Программа по Китаю и трансформационному экспорту: Поддержка искусственного интеллекта (последний доступ к февр. 16, 2021), https://www.exim.gov/who-we-serve/external-engagement/supporting-us-artificial-intel-exports; Пресс-релиз, Экспортно-Импортный банк США, Правление ЭКСИМ Единогласно одобряет Историческую Политику поддержки американских экспортеров, конкурирующих с Китайской Народной Республикой (18 декабря 2020 г.), https://www.exim.gov/news/exim-board-unanimously-approves-historic-policy-support-exporters-competing-peoples-republic; Глобальная инициатива по устойчивости инфраструктуры, Агентство США по торговле и развитию (последний доступ 16 февраля 2020 года), https://ustda.gov/call-for-initial-proposals/; Информационный бюллетень по Индо-Тихоокеанской стратегии на 2021 год, Агентство США по торговле и развитию (последний доступ 16 февраля 2020 года), https://ustda.gov/wp-content/uploads/2021-Indo-Pacific-Strategy-Fact-Sheet.pdf; Пресс-релиз Агентства США по торговле и развитию, USTDA объявляет о Цифровой стратегии 2021 года для Индо-Тихоокеанского региона (27 октября 2020 года), https://ustda.gov/ustda-announces-2021-digital-strategy-for-the-indo-pacific/.

Ссылки и ресурсы

1. Более подробную информацию о Национальной технологической стратегии см. в главе 9 настоящего доклада.

2. Более подробную информацию см. в главе 9 настоящего доклада.

3. См. Промежуточный отчет и рекомендации за третий квартал, NSCAI at 214-218 (Oct. 2020), https://www.nscai.gov/previous-reports/.

4. Комиссия поддерживает эти усилия и далее призывает правительство США активно участвовать с помощью «мозаичного подхода» для обеспечения того, чтобы Формирующаяся технологическая коалиция была аддитивной, а не дублирующей. См. Промежуточный отчет и рекомендации за третий квартал, NSCAI at 185 (октябрь 2020 г.), https://www.nscai.gov/previous-reports/.

5. Ключевых организаций для членства включают ОЭСР, Совет Европы (через Специальный комитет по ИИ), коалицию Freedom Online, GPAI и Организацию Североатлантического договора. Соединенным Штатам и другим основным государствам-партнерам следует рассмотреть вопрос о включении в качестве наблюдателей международных организаций (например, Всемирного банка, Международного валютного фонда, Всемирной организации интеллектуальной собственности, Всемирной организации здравоохранения, Всемирной торговой организации и Организации Объединенных Наций по вопросам образования, науки и культуры).

6. Рекомендация Совета по искусственному интеллекту ОЭСР (21 мая 2019 года), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

7. IDDI должна мобилизовать финансовые ресурсы и технические экспертные знания, поскольку Альянс DFI, партнерство между Американской Международной финансовой корпорацией развития и финансовыми институтами развития (DFIS) 15 других стран ОЭСР, начал действовать в ответ на COVID-19. См. Финансовые институты развития Объединяют усилия для реагирования на COVID-19 в Развивающихся странах, Американская Международная финансовая корпорация развития (6 апреля 2020 года), https://www.dfc.gov/media/press-releases/development-finance-institutions-join-forces-respond-covid-19-developing.

8. Глобальный инфраструктурный центр прогнозирует потребность в инвестициях в глобальную телекоммуникационную инфраструктуру на уровне 8,9 трлн долл.в течение следующих примерно 20 лет, при этом текущие тенденции не дотягивают до этой потребности на 1 трлн долл. Прогнозирование потребностей и пробелов в инвестициях в инфраструктуру, Глобальный инфраструктурный хаб (2020), https://outlook.gihub.org/. По оценкам Альянса за доступный Интернет, достижение всеобщего подключения к качественному широкополосному Интернету обойдется в 428 миллиардов долларов и до 10 лет. См. Майко Накагаки, Инвестиции в размере 428 миллиардов долларов, необходимые для подключения всего человечества к Интернету к 2030 году, Альянс за доступный Интернет (17 сентября 2020 года), https://a4ai.org/428-billion-investment-needed-to-connect-all-of-humanity-to-the-internet-by-2030/.

9. Это может включать двусторонние финансовые институты развития (ДФР) в странах-членах ОЭСР и многосторонние ДФР, которые являются подразделениями частного сектора межгосударственных МФУ. См. Финансовые институты развития и развитие частного сектора, ОЭСР (последний доступ 27 января 2021 года), https://www.oecd.org/development/development-finance-institutions-private-sector-development.htm.

10. См. План действий в главе 7 и Приложение к настоящему докладу, содержащее сокращенную версию Ключевых соображений NSCAI по ответственному развитию и внедрению ИИ. Дополнительные сведения о рекомендации Комиссии использовать технологии и оперативную политику, которые согласуются с сохранением конфиденциальности, см. в разделе «Приведение систем и видов использования в соответствие с американскими ценностями и верховенством закона» в разделе «Ключевые соображения ответственного развития и внедрения искусственного интеллекта: Расширенная версия», NSCAI (2021) (имеется в архиве Комиссии).

11. Принципы G20 для качественных инвестиций в инфраструктуру (последний доступ 4 января 2021 года), https://www.mof.go.jp/english/international_policy/convention/g20/annex6_1.pdf.

12. «Цифровые принципы были впервые созданы в консультации с такими организациями, как Фонд Билла и Мелинды Гейтс, Шведское агентство международного развития (SIDA), Детский фонд ООН (ЮНИСЕФ), Программа развития ООН (ПРООН), Всемирный банк, Агентство США по международному развитию (USAID) и Всемирная организация здравоохранения (ВОЗ).» См. Часто задаваемые вопросы, Принципы цифрового развития (последний доступ 3 января 2021 года), https://digitalprinciples.org/about/.

13. Критерии безопасности и доверия в Телекоммуникационных сетях и услугах, Рабочая группа CSIS по доверию и безопасности в сетях 5G (май 2020 г.), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200511_Lewis_5G_v3.pdf.

14. Рекомендация Совета по цифровой безопасности критической деятельности ОЭСР (12 октября 2019 г.), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456.

15. Руководящие принципы ОЭСР для многонациональных предприятий, OECD (2011), http://www.oecd.org/daf/inv/mne/48004323.pdf.

16. Руководящие принципы предпринимательской деятельности и прав человека: Осуществление Рамочной программы Организации Объединенных Наций «Защита, уважение и средства правовой защиты», Управление Верховного комиссара Организации Объединенных Наций по правам человека (2 011), https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf. В ознаменование 10-й годовщины принятия Руководящих принципов ООН по предпринимательству и правам человека (UNGPS) ООН рассмотрит существующие пробелы и разработает дорожную карту на следующее десятилетие. См. Руководящие принципы ООН: Следующее десятилетие,

Ресурсный центр по вопросам бизнеса и прав человека (последний доступ-февраль. 8, 2021), https://www.business-humanrights.org/en/big-issues/un-guiding-principles-on-business-human-rights/un-guiding-principles-the-next-decade/.

17. Стандарты финансирования развития, ОЭСР (последний доступ 27 января 2020 г.), http://www.oecd.org/dac/financing-sustainable-development/development-finance-standards/; Списки кодов КСР и CRS, ОЭСР (последний доступ к ним был получен 28 декабря 2020 года), http://www.oecd.org/dac/financing-sustainable-development/development-finance-standards/dacandcrscodelists.htm.

18. Рекомендация Совета по искусственному интеллекту ОЭСР (21 мая 2019 года), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

19. См. Приложение к настоящему отчету, содержащее сокращенную версию ключевых соображений NSCAI по ответственной разработке и внедрению ИИ. Дополнительные сведения см. в разделе Ключевые соображения для ответственного развития и внедрения искусственного интеллекта: Расширенная версия, NSCAI (2021) (в файле Комиссии).

20. Дополнительные сведения и рекомендации, касающиеся контроля за экспортом конечного использования и конечного пользователя, см. в главе 14 настоящего доклада.

21. Например, Hillhouse Capital, ориентированная на Азию частная инвестиционная компания, известная своими ранними инвестициями в Tencent и Baidu, выросла из «бутик-хедж-фонда « в гиганта стоимостью 60 миллиардов долларов, который делал провидческие ставки на акции, частные акции и венчурный капитал.» В настоящее время Хиллхаус стремится поднять «то, что было бы крупнейшим в Азии США». деноминированный в долларах фонд, нацеленный на 13 миллиардов долларов.» См. Michael McDonald & Lulu Yilun Chen, Hillhouse Reloads After Building $60 Billion Asia Juggernaut, Bloomberg (28 апреля 2020 г.), https://www.bloomberg.com/news/articles/2020-04-27/yale-s-2-4-billion-profit-machine-hillhouse-ready-to-reload; Kane Wu & Julie Zhu, Exclusive: Hillhouse Нацелена на более чем 3 миллиарда долларов для Нового фонда,

номинированного в юанях: Источники, Reuters (18 сентября 2020 года), https://www.reuters.com/article/us-hillhouse-fundraising-exclusive/exclusive-hillhouse-targets-over-3-billion-for-new-yuan-denominated-fund-sources-idUSKBN2690LK.

22. Рекомендации по укреплению государственно-частного партнерства и инвестиций частного сектора в Соединенных Штатах см. в главах 11, 13, 14 и 16 настоящего доклада вместе с соответствующими Планами действий.

23. Промежуточный отчет и рекомендации за третий квартал, NSCAI at 205 (октябрь 2020 г.), https://www.nscai.gov/previous-reports/.

24. Этот указ будет основываться на Указе 13859. Трамп, Исполнительный указ о сохранении американского лидерства в области искусственного интеллекта, Белый дом (11 февраля 2019 года), https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/; см. также Промежуточный отчет и рекомендации за третий квартал, NSCAI at 207-12 (Oct. 2020), https://www.nscai.gov/previous-reports/.

25. Промежуточный отчет и рекомендации за третий квартал, NSCAI at 206 (октябрь 2020 г.), https://www.nscai.gov/previous-reports/.

26. См. Приложение к главе 15 «План действий». Дополнительные рекомендации о том, как NIST может поддерживать квалифицированную уверенность в моделях ИИ и прогнозируемых результатах, см. в главе 7 настоящего доклада и связанном с ним Плане действий.

План действий: Глава 15 - Концевые примечания

27. Это включает в себя Американский национальный институт стандартов, основную отраслевую организацию, выступающую за американские компании перед международными органами по стандартизации, и Международный консультативный комитет по цифровой экономике и телекоммуникациям (IDET). См. Промежуточный отчет и рекомендации за третий квартал, NSCAI at 208-209 (октябрь 2020 г.); О IDET, Госдепартамент

США (последний доступ 11 февраля 2021 г.), https://www.state.gov/international-digital-economy-and-telecommunication-advisory-committee/about-idet/.

28. Промежуточный отчет и рекомендации за третий квартал, NSCAI at 206 (октябрь 2020 г.), https://www.nscai.gov/previous-reports/.

29. Id.

30. Id.

31. Целевая группа должна также оценивать усилия по продвижению целевых приоритетов в области развития. Например, Power Africa-это «партнерство под руководством правительства США, координируемое USAID, которое объединяет коллективные ресурсы более чем 150 партнеров государственного и частного секторов для удвоения доступа к электроэнергии в странах Африки к югу от Сахары.» См. Power Africa, USAID (30 ноября 2020 г.). https://www.usaid.gov/sites/default/files/documents/power-africa-fact-sheet-11-2020.pdf.

32. Эта оценка должна включать пересмотр Закона об оборонном производстве (DPA) как инструмента для DFC и потенциально других агентств по продвижению промышленной базы США, как это было сделано в рамках ответа на COVID-19. См. Закон об оборонном производстве (DPA), Американская Международная финансовая корпорация развития (последний доступ 4 января 2021 года), https://www.dfc.gov/dpa.

33. Цифровая стратегия включает в себя ряд взаимодополняющих усилий, связанных с подключением, кибербезопасностью, цифровыми финансами, инклюзивностью и другими областями, такими как Партнерство в области цифровых подключений и кибербезопасности, Цифровые финансы, Цифровая инклюзия, Геопространственные технологии и аналитика, Информатика развития и Цифровое сельское хозяйство. Важнейшие компоненты Цифровой стратегии также включают каталитическое финансирование миссий (Фонд цифровой экосистемы) и проведение Страновых оценок цифровой экосистемы (ДЕКА). См. Цифровую стратегию USAID на 2020-2024 годы, USAID (июнь 2020 года), https://www.usaid.gov/usaid-digital-strategy. USAID также

опубликовало ресурсы, отражающие Цифровую стратегию и описывающие демократические принципы внедрения этих технологий. См., например, Amy Paul, et al., Reflecting the Past, Shaping the Future: Making AI Work for International Development, USAID (2 мая 2019), https://www.usaid.gov/sites/default/files/documents/15396/AI-мл-in-Development.pdf; Искусственный интеллект в глобальном здравоохранении: Определение коллективного пути вперед, USAID (2020), https://www.usaid.gov/sites/default/files/documents/1864/AI-in-Global-Health_webFinal_508.pdf.

34. Например, USAID может захотеть изучить возможность того, чтобы все его программы включали минимальный порог цифрового программирования (например, 10% программных усилий включают элемент цифрового развития) в качестве ключевого элемента поддержки стран на их пути к самообеспеченности.

35. Дорожная карта воздействия, DFC (последний доступ 25 ноября 2020 года), https://www.dfc.gov/roadmap-for-impact[далее-Дорожная карта воздействия DFC].

36. Дорожная карта DFC для воздействия на 6.

37. DFC Roadmap for Impact at 57; Обоснование бюджета Конгресса: 2021 финансовый год, DFC (последний доступ 25 ноября 2020 года), https://www.dfc.gov/sites/default/files/media/documents/FY2021_DFC_CBJ-Final-04222020.pdf [далее-Бюджет DFC на 2021 финансовый год].

38. Китайский банк развития и Китайский Эксимбанк предоставляют льготные кредиты, включая, например, 40-летний льготный кредит Индонезии для финансирования ее высокоскоростной железной дороги стоимостью 5,29 млрд. Кредит предусматривал 10-летний льготный период, отсутствие гарантий со стороны Индонезии и гарантии местного содержания. См. Китайскую инициативу «Пояс и путь» в глобальной торговле, инвестициях и финансах, ОЭСР, 18 (2018), https://www.oecd.org/finance/Chinas-Belt-and-Road-Initiative-in-the-global-trade-investment-and-finance-landscape.pdf.

39. Обновление политики, Отслеживание доноров (23 июля 2020 года), https://donortracker.org/policy-updates/european-investment-bank-provide-us84-million-concessional-loan-senegal-support; Японские льготные кредиты ОПР, Организация Объединенных Наций (последний доступ к ним был получен 2 февраля 2021 года), https://www.un.org/ldcportal/japanese-concessional-oda-loans/; Понимание инфраструктурных проектов Китая «Пояс и дорога» в Африке, Брукингский институт (сентябрь 2019 года), https://www.brookings.edu/wp-content/uploads/2019/09/FP_20190930_china_bri_dollar.pdf.

40. DFC имеет официальные отношения с международными партнерами, такими как Япония и Австралия (Japan Bank for International Cooperation, Nippon Export Investment Insurance, Australia Infrastructure Financing Facility), Африканский банк развития и Межамериканский банк развития. См. Показания Адама С. Болера, генерального директора Американской Международной финансовой корпорации развития, перед Подкомитетом по ассигнованиям Палаты представителей по государственным и иностранным операциям и связанным с ними программам (4 марта 2020 года), https://www.dfc.gov/testimony-DFC-HAP-03042020.

41. Смешанное финансирование, по мнению ОЭСР, «представляет собой стратегическое использование финансирования развития для мобилизации дополнительных финансовых ресурсов на цели устойчивого развития в развивающихся странах.» Смешанное льготное финансирование включает в себя «использование относительно небольших объемов льготных донорских средств для смягчения конкретных инвестиционных рисков и содействия сбалансированию профилей риска и вознаграждения новаторских инвестиций, которые не могут осуществляться на строго коммерческих условиях.» См. Blended Finance, OECD (последний доступ 28 декабря 2020 г.), https://www.oecd.org/dac/financing-sustainable-development/blended-finance-principles/; Смешанное льготное финансирование, Международная финансовая корпорация Группы Всемирного банка (последний доступ 28 декабря 2020 года),

https://www.ifc.org/wps/wcm/connect/topics_ext_content/ifc_external_corporate_site/bf; см. также Blended Finance, Convergence (последний доступ 28 декабря 2020 г.), https://www.convergence.finance/blended-finance.

42. Этот инвестиционный фонд можно было бы смоделировать по образцу Всемирного фонда управления банковскими активами для женщин в размере 100 миллионов долларов, который получил 25 миллионов долларов от DFC и 600 000 долларов от USAID. Кроме того, DFC объявила конкурс предложений для управляющих фондами, инвестирующих в компании, связанные с 5G, работающие в странах с формирующимся рынком, имеющих право на участие в DFC, с целью инвестирования в открытые и безопасные ИКТ. См. Первый в своем роде Смешанный финансовый фонд правительства США для расширения прав и возможностей женщин на развивающихся рынках, DFC (4 июня 2019 года), https://www.dfc.gov/media/opic-press-releases/first-its-kind-us-government-blended-finance-fund-empower-women; Конкурс предложений по информационно-коммуникационным технологиям, DFC (март 2020 года), https://www.dfc.gov/sites/default/files/media/documents/IFD_5G_CFP_032020.pdf.

43. Запрос в размере 82 миллионов долларов был частью более крупного запроса в размере 640,1 миллиона долларов, запрошенного для поддержки усилий DDI. См. Бюджетное обоснование Конгресса: Иностранные операции: Приложение 2: 2021 финансовый год, Государственный департамент США в 223 (2020), https://www.state.gov/wp-content/uploads/2021/01/FY21-CBJ-Appendix-2-FINAL-508-Version.pdf.

44. Фонд цифровой экосистемы «предоставляет Оперативным подразделениям Агентства каталитическое финансирование для разработки и осуществления мероприятий, способствующих развитию открытых, инклюзивных и безопасных цифровых экосистем. DEF поддерживает два типа вмешательств: 1) Возникающие возможности для использования или формирования цифровой экосистемы в любом секторе; 2) Стратегические инициативы по укреплению или улучшению цифровой экосистемы.» См.

Digital Ecosystem Fund: 2020 Activities, USAID (22 декабря 2020 г.), https://www.usaid.gov/digital-development/DEF2020.

45. Бюджетный запрос DFC на 2021 финансовый год предусматривал выделение таких средств в размере 700 миллионов долларов. См. Бюджет DFC на 2021 финансовый год в разделе 1.

46. Правительство США объявило о создании первого в своем роде смешанного финансового фонда в июне 2019 года. USAID предоставило 600 000 долларов финансирования и технической помощи, а предшественник DFC инвестировал 25 миллионов долларов в поддержку частных капиталовложений в Фонд управления активами Всемирного банка для женщин стоимостью 100 миллионов долларов. См. Первый в своем роде Смешанный финансовый фонд правительства США для расширения прав и возможностей женщин на развивающихся рынках, DFC (4 июня 2019 года), https://www.dfc.gov/media/opic-press-releases/first-its-kind-us-government-blended-finance-fund-empower-women; Винс Чедвик, USAID, OPIC Team Up on Women's Finance in ‘Preview’ of New DFI Era, Devex (5 июня 2019), https://www.devex.com/news/usaid-opic-team-up-on-women-s-finance-in-preview-of-new-dfi-era-95050.

47. См., например, Дорожную карту DFC для воздействия на 57.

48. Бюджет DFC на 2021 финансовый год; Дорожная карта воздействия DFC.

49. Дорожная карта DFC для воздействия на 56.

50. См. Главу 14 настоящего отчета для получения рекомендаций относительно конкретных средств контроля конечного использования высококачественных чипов ИИ.

51. 85 Fed. Reg. 43532, Advanced Surveillance Systems and Other Items of Human Rights Concern, U. S. Department of Commerce: Bureau of Industry and Security (17 июля 2020 г.), https://www.federalregister.gov/documents/2020/07/17/2020-15416/advanced-surveillance-systems-and-other-items-of-human-rights-concern; 85 Fed. Reg. 63007,

Поправка к Политике лицензирования товаров, контролируемых по соображениям борьбы с преступностью, Министерство торговли США: Бюро промышленности и безопасности (окт. 6, 2020), https://www.federalregister.gov/documents/2020/10/06/2020-21815/amendment-to-licensing-policy-for-items-controlled-for-crime-control-reasons.

План действий: Глава 15 - Концевые примечания

52. Руководство по реализации Руководящих принципов ООН для транзакций, связанных с конечными пользователями иностранных правительств для Продуктов или услуг с возможностями наблюдения, Государственный департамент США (последний доступ 4 января 2021 года), https://www.state.gov/wp-content/uploads/2020/10/DRL-Industry-Guidance-Project-FINAL-1-pager-508-1.pdf.

53. Кара Фредерик, Демократия по замыслу: Позитивный ответ на нелиберальное использование технологий на 2021 год, Центр новой американской безопасности (15 декабря 2020 года), https://www.cnas.org/publications/reports/democracy-by-design; Далия Петерсон, Разработка альтернатив репрессивному надзорному государству Китая, Центр безопасности и новых технологий (октябрь 2020 г.), https://cset.georgetown.edu/wp-content/uploads/CSET-Designing-Alternatives-to-Chinas-Surveillance-State.pdf.

54. GPAI была запущена в июне 2020 года для продвижения «ответственного и ориентированного на человека» ИИ в соответствии с правами человека, основными свободами, демократическими ценностями, инновациями и экономическим ростом. В настоящее время членами Организации являются Австралия, Бразилия, Канада, Европейский союз, Франция, Германия, Индия, Италия, Япония, Мексика, Нидерланды, Новая Зеландия, Польша, Сингапур, Словения, Южная Корея, Испания, Соединенное Королевство и Соединенные Штаты, а также ОЭСР и ЮНЕСКО в качестве постоянных наблюдателей. См. UNESCO Joins Global Partnership on Artificial Intelligence as Observer, UNESCO (Dec. 10, 2020),

https://en.unesco.org/news/unesco-joins-global-partnership-artificial-intelligence-observer.

55. Пять рабочих групп ГПАИ (ответственный ИИ, управление данными, инновации и коммерциализация, будущее работы и борьба с пандемией) поддерживаются исследованиями, проводимыми двумя экспертными центрами: Парижским Национальным институтом исследований в области цифровой науки и техники (INRIA) и Монреальским Международным экспертным центром по развитию искусственного интеллекта (ICEMAI). См. Официально запущенное Глобальное партнерство по искусственному интеллекту, Монреальский международный форум (15 июня 2020 года), https://www.montrealinternational.com/en/news/the-global-partnership-on-artificial-intelligence-officially-launched/; Запуск Глобального партнерства по искусственному интеллекту 15 членами-основателями Министерства Европы и иностранных дел Франции (15 июня 2020 года); https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/launch-of-the-global-partnership-on-artificial-intelligence-by-15-founding.

56. Работа ОЭСР через Директорат по науке, технологиям и инновациям и Обсерваторию политики ИИ поддерживается партнерскими отношениями с правительствами и исследовательскими организациями, такими как поддержка Немецкой обсерваторией ИИ усилий ОЭСР по влиянию ИИ на рынок труда. См.Программу «Работа, инновации, производительность и навыки»: Обзор, ОЭСР.AI (последний доступ 1 февраля 2021 года), https://oecd.ai/work-innovation-productivity-skills.

57. Going Digital, OECD (последний доступ 2 февраля 2021 года), http://www.oecd.org/going-digital/project/.

58. Международная исследовательская станция Банф (последний доступ 4 января 2021 года), https://www.birs.ca/.

59. AccelNet ускоряет сотрудничество между сетями, финансируя связь (путешествия, виртуальные сети, семинары) между международными

исследовательскими сетями. NSF финансирует только американскую часть и ожидает, что международные партнеры будут финансировать свою часть сотрудничества. Помимо финансирования связей между существующими сетями, AccelNet будет финансировать усилия по созданию и развитию зарождающихся сетей. См. Ускорение исследований С Помощью Международного Сотрудничества между Сетями (AccelNet), NSF (21 сентября 2020 г.), https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=505584&org=OISE&from=home.

60. МУЛЬТИПЛИКАТОР направляет предметных экспертов в международные области интересов для оценки возможностей и сбора информации для потенциальных совместных проектов NSF. Эта новая программа уже была многообещающей—NSF направила мультидисциплинарную команду в Чехию и была поражена их возможностями. В настоящее время NSF изучает возможности двустороннего сотрудничества. См. NSF MULTIPLIER: MULTIPlying Impact Leveraging International Experience in Research Missions, NSF (последний доступ 28 декабря 2020 г.), https://www.nsf.gov/od/oise/multiplier.jsp; Обсуждения сотрудников NSCAA с сотрудниками NSF (14 ноября 2020 г.).

61. Например, национальные лаборатории Министерства энергетики могут быть использованы для финансирования исследований с рекомендуемым целевым финансированием.

62. Общий исследовательский ресурс может помочь предотвратить узкие места из-за ограниченных компьютерных ресурсов. Эти усилия также могут быть, при необходимости, частью расширения Национального исследовательского ресурса по ИИ, описанного в главе 9 настоящего доклада.

63. NSCA рекомендует каждому члену выделять финансирование для поддержки исследовательских усилий. Тем не менее, MAIRI также будет служить местом для исследований, чтобы собираться для диалогов, семинаров и наставничества. Основываясь на аналогичных международных научно-

исследовательских институтах, члены MAIRI должны рассмотреть возможность предоставления эквивалента $100 тыс. - $250 тыс. в год для покрытия расходов на проезд, проживание и суточные около 80 исследователей MAIRI для облегчения коммуникации и взаимодействия между исследователями.

64. В 2017 году правительство провинции Альберта (Канада), Канадский Совет по естественным наукам и инженерным исследованиям, Национальный научный фонд США и Мексиканский Consejo Nacional de Cinco y Tecnologia инвестировали 12,5 миллиона долларов в течение следующих пяти лет. See Research Station Gets $12.5 M to Bring Scientists and Mathematics to Banff, CBC News (10 февраля 2017), https://www.cbc.ca/news/canada/calgary/banff-international-research-station-math-science-funding-1.3977703. За период 2012-2017 годов ЗАЯВКИ получили $10,3 млн, из которых $3,68 млн-от NSF. За период 2006-2011 годов заявки получили 9,3 миллиона долларов, из которых 3,1 миллиона долларов-от NSF. См. Организацию: Международная исследовательская станция Банф, Research Money (последний доступ 4 января 2021 года), https://researchmoneyinc.com/organization/banff-international-research-station/.

65. Национальные научно-исследовательские институты ИИ представляют собой важный пример использования возможностей сотрудничества в области НИОКР в рамках межведомственного сотрудничества США. Новые центры NSF и DOE по квантовой информатике также являются ярким примером преимуществ выделенных ресурсов и приоритизации между двумя исследовательскими организациями правительства США. См. Андреа Петерсон, NSF и DOE Поддерживают исследовательские приоритеты с помощью Spate of New Center Awards, American Institute of Physics (16 сентября 2020 г.), https://www.aip.org/fyi/2020/nsf-and-doe-support-research-priorities-spate-new-center-awards.

Дополнительные сведения

7 Визы J-1 используются академическими работодателями, такими как университеты и исследовательские институты, для спонсирования иностранных ученых, стажеров, стажеров и исследователей для работы в течение нескольких месяцев или пяти лет в Соединенных Штатах. Владельцы виз J-1 не имеют права продлевать свои визы и должны ждать от одного до двух лет, прежде чем они смогут подать заявление на другой иммиграционный статус. Визы O-1 предназначены для лиц, которые могут предоставить обширные доказательства того, что они обладают «экстраординарными способностями в области науки, искусства, образования, бизнеса или легкой атлетики.» Эти визы длятся до трех лет с бессрочным продлением, но использовались минимально для привлечения экспертов в области науки и техники из-за ограничительных политических указаний. Обсуждение иммиграционных и визовых программ для привлечения ученых и исследователей в Соединенные Штаты см. в общем виде Zachary Arnold, et al., Immigration Policy and the U. S. AI Sector, CSET (Sept. 2019), https://cset.georgetown.edu/research/immigration-policy-and-the-u-s-ai-sector/.

68. См. также главу 1 настоящего отчета о злонамеренных информационных операциях.

69. Госсекретарь Помпео утверждает Новое Бюро по безопасности киберпространства и новым технологиям Госдепартамента США (7 января 2021 года). https://2017-2021.state.gov/secretary-pompeo-approves-new-cyberspace-security-and-emerging-technologies-bureau//index.html.

70. Дополнительные сведения о функциях и потребностях КРЕДИТНОГО бюро см. в Рекомендациях за второй квартал, NSCAI at 88-89 (июль 2020 г.), https://www.nscai.gov/previous-reports/.

71. Эти элементы должны включать ключевые, связанные с технологией функции предлагаемого Бюро CSET; Бюро океанов, окружающей среды и науки (OES); Бюро советника Секретаря по науке и технике (STAS); Координатора по кибернетическим вопросам (S/CCI); Бюро по экономическим

и деловым вопросам (EB); Бюро по демократии, правам человека и труду (DRL); и Центр аналитики.

72. Ключевые темы, Офис советника по науке и технологиям Государственного департамента США (последний доступ 15 декабря 2020 года), https://www.state.gov/key-topics-office-of-the-science-and-technology-advisor/.

73. Дипломаты в резиденции Госдепартамента США (последний доступ 2 февраля 2021 года), https://careers.state.gov/connect/dir/.

74. См., например, Управление американскими пространствами, Госдепартамент США (последний доступ 1 февраля 2021 года), https://americanspaces.state.gov/; TechCamp, Государственный департамент США (последний доступ 1 февраля 2021 года), https://techcamp.america.gov/; Описание программы, World Learning (последний доступ 1 февраля 2021 года), https://www.worldlearning.org/program/u-s-speaker-program/.

75. См. О GIST, GIST (последний раз обращался 1 февраля 2021 года), https://www.gistnetwork.org/about.

Благоприятный международный технологический порядок

Коалиция зарождающихся технологий

В настоящем приложении излагаются рамки и всеобъемлющая повестка дня глобального сотрудничества в области искусственного интеллекта (ИИ) и новых технологий. Она включает в себя руководство по конкретным оперативным проектам, приложениям и механизмам реализации совместной работы ИИ в семи важнейших областях. Совместная работа в этих областях будет способствовать дальнейшему развитию ИИ в соответствии с демократическими ценностями и укреплению связей, связывающих Соединенные Штаты с их союзниками и партнерами. Настоящее приложение предназначено для предоставления руководящих указаний Формирующейся

технологической коалиции (ИТК) и может помочь должностным лицам в определении приоритетов двусторонних и многосторонних совместных усилий вне контекста, включая участие в многосторонних инициативах по всему ландшафту ИИ.

• *Цели:*

Продвигать общие демократические нормы и ценности для управления и руководства ответственным искусственным интеллектом (ИИ), а также исследованиями, разработками и применением новых технологий во всем мире.

Продвигать международные нормы и стандарты ИИ, поддерживающие демократические ценности, опираясь на руководящие документы, такие как Организация экономического сотрудничества и развития (ОЭСР) Принципы ИИ и усилия по практической реализации принципов, отраженные в Ключевых соображениях Комиссии по ответственному развитию и внедрению искусственного интеллекта.

Координировать позиции правительственных делегаций государств-партнеров и, в соответствующих случаях, национальных (неправительственных) институтов по стандартизации, аккредитованных при международных организациях по техническим стандартам, в целях поддержки разработки безопасных, надежных и надежных технологий и обеспечения этической и технической целостности, утверждения стандартов, соответствующих демократическим ценностям, и поддержания нейтралитета этих организаций.

• Приоритетные области координации.

ЭТП должна стремиться к согласованию с союзниками и партнерами и приоритизации усилий по разработке международных технических стандартов в следующих приоритетных областях:

Безопасность и надежность;

Технологии повышения конфиденциальности, включая машинное обучение с сохранением конфиденциальности (PPмл), объединенный криптографический код и другие технологии повышения конфиденциальности;

Обмен данными, маркировка и соответствующая документация для данных, моделей и систем;

Оценка производительности системы и характеристика «слепых зон» в соответствии с общими ценностями (включая справедливость, интерпретируемость, надежность и безопасное использование технологий искусственного интеллекта в составе интегрированных систем);

Робастность, обеспечивающая устойчивость моделей к враждебным примерам и инверсии моделей, в то время как красные объединяются с союзниками в попытках конкурентов подорвать системы с поддержкой искусственного интеллекта;

Доверие к человеко-машинному объединению и разработке единых стандартов и критериев оценки рисков в условиях различной сложности и неопределенности;

Прослеживаемость, ориентированная на требования аудиторского следа и требования к разрешениям для систем искусственного интеллекта с высокими ставками, включая критически важные для безопасности приложения; и

Интероперабельность, включая контрольные показатели, оценивающие надежность полученных модельных объяснений.

• Механизмы координации.

В дополнение к координации усилий через ИТП правительство США, возглавляемое Государственным департаментом и в координации с Национальным институтом стандартов и технологий (NIST) и его координатором по стандартам ИИ, должно взаимодействовать с демократическими странами для согласования позиций по стандартам, которые имеют решающее значение для взаимной безопасности и обороны.

Государственный департамент, как это было рекомендовано Комиссией, находится в процессе размещения региональных технических сотрудников в крупных зарубежных технологических центрах. Такое развитие событий будет способствовать дипломатическим усилиям по согласованию позиций с союзниками и партнерами.

Как Комиссия рекомендовала в своих Рекомендациях6 за третий квартал и в других разделах настоящего Доклада, НИСТ и другие учреждения должны рассмотреть Ключевые соображения Комиссии по ответственной разработке и внедрению ИИ. Ключевые соображения включают оперативное руководство по стандартам, имеющим решающее значение для ответственного ИИ и национальной безопасности, в том числе по техническим стандартам тестирования и оценки, верификации и валидации (TEVV).

Координация по техническим стандартам должна включать работу международных организаций по стандартизации, а также скоординированную работу по введению в действие норм и принципов ИИ. Рабочая группа по управлению данными Глобального партнерства по ИИ (GPAI) может предоставить особенно заметные передовые практики для разработки и реализации инициатив по обмену данными, объединению и сбору данных.8 ОЭСР также является важнейшим форумом для разработки технических стандартов и руководящих принципов, особенно в области обмена данными и ответственного ИИ.

Критическая область № 2 – Совместные исследования и разработки в области ИИ и цифровой инфраструктуры

• Цели:

Определите области общих интересов, способствующие совместным НИОКР, такие как технологии повышения конфиденциальности, подходы к использованию малых данных в ИИ, материалы следующего поколения, прототипирование и высокопроизводительные вычисления (HPC), для которых существуют существующие пробелы, и определите способы совместного использования ресурсов для проведения НИОКР в этих областях.

Разработать механизмы содействия фундаментальным и прикладным научно-исследовательским проектам, предполагающим сотрудничество между странами, отраслевыми партнерами и исследователями.

Проекты могут также включать безопасные облачные фреймворки, обмен передовым опытом в области TEVV, инновационные модели финансирования, международные испытательные стенды для разработки докоммерческих технологий и использование предлагаемого Комиссией Многостороннего исследовательского института ИИ для

Продолжайте совместные, скоординированные усилия по разработке и развертыванию приложений искусственного интеллекта на благо человечества в целом в областях, представляющих глобальный интерес, таких как те, которые воплощены в Целях устойчивого развития ООН.

• Приоритетные направления совместных НИОКР—развитие технологий ИИ.

Разработка технологий сохранения конфиденциальности, таких как гомоморфное шифрование и методы дифференциальной конфиденциальности, для облегчения трансграничных приложений искусственного интеллекта, обмена данными и совместных усилий.

Непрерывное развитие и адаптация систем TEVV для укрепления развития надежного и надежного ИИ имеет решающее значение для продвижения интересов демократических стран и понимания того, как системы ИИ работают в условиях мультиагентности/состязательности. Сотрудничество в этой области будет способствовать пониманию различий между союзниками в политике, показателях, стандартах и требованиях, создавая при этом более прочные связи для всех пользователей в рамках подхода полного цикла.

Разработка ИИ для моделирования, моделирования и проектирования, чтобы предоставить исследователям более широкий спектр готовых к ИИ наборов данных.

Разработка алгоритмов обучения с одним и несколькими выстрелами - алгоритмов, которые полагаются на меньшее количество данных,-чтобы

облегчить будущие совместные исследования и разработки и обмен данными и улучшить контекстно-специфическую совместимость.

Разработка надежного союзного ИИ для снижения уязвимости союзных систем ИИ и обучающих данных к атакам противника.

Достижение контекстно-специфической интероперабельности систем ИИ, необходимой для трансграничных приложений ИИ, с акцентом на то, как системы интегрируют конкретные компоненты ИИ/ML. Потенциал ИИ для повышения скорости операций потребует от союзников и партнеров стресс-тестирования процедур принятия решений и коммуникационных протоколов для обеспечения совместимости. Интероперабельность систем искусственного интеллекта уже является проблемой на переднем крае оборонного сотрудничества и будет только возрастать по мере развития технологий.

Разработка ИИ для обеспечения и повышения устойчивости цепочек поставок для защиты цепочек поставок компонентов ИИ при одновременном продвижении внутренних и смежных инноваций, а также для применения ИИ для улучшения аудита, картографирования и обеспечения безопасности цепочек поставок при одновременном обеспечении устойчивости к шокам. Учитывая изначально трансграничный характер цепочек поставок и их критическую роль в международной экономике вокруг ИИ и передовых технологий, это естественная область для сотрудничества Соединенных Штатов с государствами-единомышленниками.

Дополнительные критические области исследований ИИ, включая новые направления машинного обучения (ML), сложные мультиагентные сценарии, расширенное понимание сцены, оценку рисков системы ИИ, расширенное взаимодействие человека и ИИ и объединение в команды, а также автономные системы ИИ.

• Приоритетные направления совместных НИОКР—ИИ на благо человечества. Потенциал ИИ для оказания помощи мировому сообществу в улучшении условий жизни людей огромен. Приоритетными направлениями международного сотрудничества должны быть следующие:

Окружающая среда и климат. Признавая растущее мнение о том, что деградация окружающей среды и изменение климата представляют собой императивы национальной и международной безопасности, международное сообщество должно совместно работать над разработкой решений на основе искусственного интеллекта для решения общих климатических, экологических и энергетических проблем.

Совместные инициативы, такие как следующие, служат образцами для будущих международных усилий:

• Партнерство между Рабочей группой по Кросс-секционной оценке и Рабочей группой Агентства по атомной энергии ОЭСР (АЯЭ) по международной оценке ядерных данных Сотрудничество в рамках Проекта Международной оценки критичности и безопасности;

• ГЕОТЕРМИКА-сотрудничество между 12 европейскими странами и Соединенными Штатами для финансирования специфических исследований ИИ в области геотермальных НИОКР;

• Международное партнерство по водороду и топливным элементам в экономике (IPHE) - межправительственное партнерство по содействию и ускорению перехода к чистой и эффективной энергетике при поддержке исследований в области искусственного интеллекта и ОД.

Здравоохранение, включая выявление пандемий и реагирование на них. Кризис COVID-19 ясно показал необходимость глобального сотрудничества и потенциал решений с использованием ИИ.

Умный мониторинг заболеваний. Комиссия рекомендовала глобальное сотрудничество в области интеллектуального мониторинга заболеваний. Такая глобальная инициатива, например, могла бы быть направлена на объединение существующих данных о зоологических разливах с данными из открытых источников, связанными со здоровьем, для создания общих, прогностических моделей глобального мониторинга заболеваний.

Готовность к пандемии, разработка вакцин и синдромный надзор. Усилия в этом направлении включают в себя:

• Разработка и координация международных норм и стандартов, регулирующих использование и обмен международными медицинскими данными, защита конфиденциальности при одновременном обеспечении своевременной доступности данных;

• Разработка стандартов конфиденциальности наборов геномных данных;

• Расширение международного сотрудничества в рамках Консорциума высокопроизводительных вычислений COVID-19 (потенциально через GPAI);

• Содействие международному сотрудничеству с работой DARPA по созданию инфраструктуры и протоколов для обмена данными и сотрудничества на этапе экспериментов по открытию лекарств.

Инициативы, направленные на обеспечение долгосрочного качества жизни. Сотрудничество с союзниками и партнерами может способствовать рекомендованному Комиссией сосредоточению внимания на использовании ИИ, чтобы помочь пожилым людям жить независимо дольше, помочь в управлении здоровьем и повседневными задачами, а также улучшить качество жизни, особенно за счет применения ИИ в биомедицине.

Исследовательские сообщества США-ЕС Национальной нанотехнологической инициативы, наряду с различными усилиями стран-партнеров на национальном уровне, должны служить образцами для более масштабного международного сотрудничества.

Продовольственная безопасность. Соединенные Штаты в своих программах внешней помощи уделяют особое внимание экономическому росту, устойчивости, питанию и водной безопасности, санитарии и гигиене. Укрепление безопасности воды и продовольствия стран-партнеров необходимо для того, чтобы разорвать порочный круг нищеты, голода и конфликтов.

Сельскохозяйственные отрасли все шире используют технологии, основанные на данных, такие как робототехника, спутники, GPS и беспилотные летательные аппараты. Создаются значительные массивы данных о росте сельскохозяйственных культур, характеристиках почвы и погодных условиях.

Алгоритмы на основе ИИ и мл могут усилить наборы данных и аппаратное обеспечение для улучшения мониторинга и анализа сельскохозяйственных и распределительных процессов в реальном времени. Это может улучшить усилия по оценке потребностей, повышению производительности и безопасности, а также наращиванию местного потенциала и производительности при минимизации воздействия на окружающую среду.

Помощь в случае стихийных бедствий. Технологии с поддержкой искусственного интеллекта используются для решения целого ряда сценариев стихийных бедствий, и следует изучить возможность дальнейшей работы на международной основе. Всемирный экономический форум входит в число тех групп, которые призывают к расширению международного сотрудничества в целях реализации преимуществ ИИ, особенно в области оказания помощи в случае стихийных бедствий.

Стихийные бедствия, связанные с климатом и погодой, такие как ураганы, лесные пожары и наводнения, находятся на подъеме, и ИИ уже применяется для смягчения последствий, обнаруживая выживших с помощью беспилотных летательных аппаратов, удаляя мусор после катастрофы, развертывая роботов для связи с жертвами, используя передовые технологии для получения самых современных данных, выполняя прогнозное моделирование и используя репортажи в социальных сетях.

Министерство обороны сотрудничает с DoE и Microsoft в разработке «алгоритмов глубокого обучения искусственного интеллекта для предоставления данных почти в реальном времени для улучшения принятия решений первыми лицами, участвующими в ликвидации последствий стихийных бедствий и оказании гуманитарной помощи», и такие страны, как Сингапур, работают с Объединенным центром искусственного интеллекта (JAIC) над этой конкретной Национальной инициативой миссии.

Соединенные Штаты могут работать со своими союзниками и партнерами для эффективного прогнозирования, моделирования, подготовки к бедствиям и

реагирования на них, как рекомендует Комиссия в главе 11 настоящего доклада.

Гражданское космическое сотрудничество. Соединенные Штаты и другие космические агентства используют искусственный интеллект для решения целого ряда космических задач, включая визуализацию космических объектов и ситуационную осведомленность, отслеживание космического мусора для предотвращения столкновений со спутниками, блуждание по лунной поверхности, исследование глубокого космоса с помощью автономных систем и обнаружение астероидов, которые могут угрожать Земле.

Для безопасной спутниковой навигации вокруг космического мусора Европейское космическое агентство (ЕКА) и Британское космическое агентство реализуют инициативы в области искусственного интеллекта, что предполагает потенциальные возможности для более тесного сотрудничества США. ЕКА уже установило партнерские отношения со Стэнфордом.

Индия также строит свою космическую программу и развернула луноход с искусственным интеллектом.

Россия и Китай, по-видимому, разрабатывают технологические решения проблемы космического столкновения, которые могли бы стать областью взаимовыгодного сотрудничества. Роботизированные помощники с поддержкой искусственного интеллекта также разрабатываются для Международной космической станции.

• Методы реализации совместных НИОКР. ИТЦ также следует изучить механизмы, позволяющие осуществлять сотрудничество в области НИОКР между правительственными партнерами и неправительственными организациями.

Сотрудничество должно включать не только межведомственные усилия, но и методы партнерства с исследователями в академических исследовательских центрах и в частном секторе.

Существующие соглашения между правительствами в области науки и техники (НИОКР) могут служить правовой основой для сотрудничества, но детали будут зависеть от рассматриваемой договоренности.

ИТЦ должен уделять приоритетное внимание подходам, которые будут способствовать объединению ресурсов, сокращению избыточности и поддержке разработки и обобщения передового опыта.

Кроме того, ИТЦ следует изучить проблемы, связанные с трансграничными совместными НИОКР-например, связанные с конфиденциальностью данных и обменом данными между Соединенными Штатами и Европейским Союзом, и изучить решения для преодоления этих проблем.

• Потенциальные методы осуществления и дальнейшего сотрудничества в области НИОКР включают:

Создание Многостороннего научно-исследовательского института искусственного интеллекта (МИРИ). Предложенный Комиссией в настоящем докладе, MAIRI будет служить центром многосторонних исследований для координации совместных усилий по разработке технологий и согласованию норм, способствующих развитию ответственного, ориентированного на человека и сохраняющего конфиденциальность ИИ/ОД, который улучшает общество.

Определение приоритетов научно-исследовательской работы Глобального партнерства по ИИ (ГПАИ). ИТЦ должен использовать существующие рамки везде, где это возможно, и GPAI, поддерживаемая в настоящее время Канадским Международным экспертным центром по развитию искусственного интеллекта в Монреале (ICEMAI) и Французским Национальным институтом исследований в области цифровой науки и техники (INRIA), является одной из наиболее перспективных многосторонних инициатив с участием многих заинтересованных сторон по проведению совместных НИОКР и продвижению технологий искусственного интеллекта для общих целей. Комиссия предложила большую роль для США.

исследователи через базирующийся в США Экспертный центр, используя Национальные исследовательские институты ИИ NSF.

Создание совместного инвестиционного консорциума развивающихся технологий. По образцу In-Q-Tel консорциум будет стимулировать инвестиции Соединенных Штатов и иностранных партнеров в компании на ранних стадиях развития для дальнейшего развития технологий искусственного интеллекта, которые продвигают и/или защищают демократические ценности. Эти усилия принесут пользу Соединенным Штатам и их союзникам и партнерам через трансграничную платформу для взаимодействия со стартапами и предпринимателями в области искусственного интеллекта и новых технологий.

В рамках правительства США эти усилия должны опираться на региональных технических сотрудников Госдепартамента, Внешнеторговую службу и миссии USAID для выявления НИОКР и прототипов для продвижения дипломатических, исследовательских и коммерческих интересов США.

Запуск многосторонних конкурсов инновационных премий. По образцу конкурсов Агентства перспективных оборонных исследовательских проектов (DARPA) и Фонда XPRIZE международные конкурсы инновационных премий, спонсируемые двумя или более правительствами, стимулировали бы исследования и разработки в области фундаментального ИИ или вокруг конкретных приложений, необходимых для национальной безопасности, и помогали бы объединять ресурсы и таланты с союзниками и промышленностью.

Содействие союзническим исследованиям в национальных лабораториях США. ИТЦ должен рассмотреть рекомендации по расширению исследований союзников (потенциально подмножества членов ИТЦ) в национальных лабораториях США по чувствительным темам. Хотя в национальных лабораториях США существуют ограничения на допуск иностранных исследователей, внутренние исследовательские усилия ограничат озабоченность по поводу трансграничного обмена данными и

кибербезопасности и могут оказаться плодотворными в области исследований и разработок, необходимых для применения в области обороны и безопасности.

Разработка платформы согласования НИОКР и глобальной системы сканирования горизонта. Платформа будет связывать исследователей и их проекты с спонсорами и партнерами (правительствами, филантропами, венчурными капиталистами, компаниями, исследовательскими институтами), обеспечивая правительству США более широкую видимость тенденций в области исследований. Возможности глобального НИОКР по сканированию горизонтов дополняли бы эти усилия и опирались бы на данные из открытых источников, чтобы дать директивным органам более глубокое понимание соответствующих открытий и ключевых тенденций в этой области.

Разработка международного испытательного стенда для ТЭВВ. Международный испытательный стенд для TEVV может быть смоделирован на базе Национальных исследовательских институтов ИИ или рекомендованного Комиссией создания спонсируемого NIST стороннего испытательного центра, но с трансграничной направленностью, а также на основе проекта AI4EU.

Улучшение сотрудничества между центрами передового опыта, научно-исследовательскими институтами и промышленными консорциумами за счет дополнительной координации со стороны правительств-партнеров. Эта концепция будет использовать существующие и вскоре созданные центры, такие как MAIRI, Центры передового опыта Европейского Союза, Европейские центры цифровых инноваций, связанные с искусственным интеллектом, США. Программа Национальных исследовательских институтов ИИ, Центр передового опыта Администрации общего обслуживания ИИ (в партнерстве с Департаментами сельского хозяйства, здравоохранения и социальных служб, а также JAIC), Институт Алана Тьюринга в Великобритании и в Канаде Монреальский институт алгоритмов обучения (Mila),46 Альбертский институт машинного интеллекта (Amii) и Векторный институт искусственного интеллекта. Со стороны США это может включать в себя развитие

промышленности и академических усилий, таких как Стэнфордский институт искусственного интеллекта, ориентированного на человека.

Содействие созданию бинациональных научно-исследовательских фондов. Члены ЕТС могут рассмотреть возможность разработки целенаправленных, бинациональных НИОКР по образцу уникальных бинациональных основ, которые облегчают американо-израильские и американо-индийские НИОКР по передовым вопросам.50 Они могут служить образцом для других союзников и партнеров для созыва международных исследователей.

Критическая область – Содействие демократии, правам человека и верховенству права

• Цели:

Совместные, скоординированные усилия по противодействию антидемократическому использованию ИИ и новых технологий посредством скоординированной политики, согласования нормативных требований (таких как экспортные ограничения конечных пользователей) и внедрения технологий.

Потенциальные приоритеты включают в себя противодействие цензуре, противодействие вредоносным информационным операциям и продвижение демократических моделей технологий наблюдения, хотя ИТП следует изучить целый ряд потенциальных применений.

Дальнейшее развитие этих нормативных приоритетов будет опираться на методы реализации, рассматриваемые в других важнейших областях, особенно № 2 (совместные НИОКР), № 5 (защита и поощрение инноваций) и № 7 (Международная инициатива цифровой демократии).

• Противодействие цензуре и авторитарному использованию технологий;

ИТЦ следует изучить усилия по использованию ИИ и связанных с ним технологий для дальнейшего расширения свободы Интернета и противодействия цензуре во всем мире. Эта работа должна быть направлена на реализацию принципов, принятых в ноябре 2020 года Коалицией Freedom

Online-партнерством 32 правительств, объединенных вокруг поощрения прав человека и индивидуальной свободы.

Соединенные Штаты должны использовать Фонд открытых технологий, созданный NDAA в 2021 финансовом году, для поддержки этих усилий, а также связанных с ними усилий Бюро по вопросам демократии, прав человека и труда (DRL) при Государственном департаменте.

ИТЦ должен координировать усилия в этом пространстве со Специальным комитетом Совета Европы по ИИ, созданным в ноябре 2019 года для сосредоточения внимания на разработке, проектировании и применении ИИ в областях прав человека, демократии и верховенства права.

Для поощрения поведения частного сектора, согласующегося с общими демократическими ценностями, ИТП следует разработать предложение о контроле за конечными пользователями, которое не стимулировало бы частные компании экспортировать ИИ и связанные с ним технологии, которые могут использоваться для подавления и нарушения прав человека и гражданских прав.

• Противодействие Вредоносным Информационным Операциям

Пагубные информационные операции представляют собой растущую международную проблему, которая усугубляется использованием технологий ИИ/мл.

Этот ИТП должен рассматривать скоординированные усилия (за пределами разведывательного пространства) по противодействию дезинформации и другим информационным операциям. Совместные усилия включают выявление, модерирование, идентификацию и классификацию вредоносной информации, разработку стандартов и передовой практики, а также подготовку экспертов.

Комиссия рекомендует создать Международную целевую группу по противодействию Дезинформации и борьбе с ней. Международная целевая группа по противодействию дезинформации и борьбе с ней (МФТ-CCAD) может быть создана в качестве совместного проекта между Соединенными

Штатами и несколькими странами, а также ЕС и НАТО для дальнейших совместных усилий по обеспечению модерации контента и обнаружению дезинформации, разработке стандартов выявления и классификации дезинформации и дезинформации (включая обнаружение глубоких подделок) и обмену передовым опытом и извлеченными уроками с союзниками. Важными партнерами в этих усилиях будут частный сектор, научные круги и организации гражданского общества.

МФТ-CCAD должна черпать передовой опыт из Глобального интернет-форума по борьбе с терроризмом и работать в координации с ним, а также с усилиями Группы по технологическому взаимодействию Центра глобального взаимодействия Госдепартамента (GEC), Целевой группы по внешнему влиянию Федерального бюро расследований (FITF), Целевой группы по стратегическим коммуникациям Европейских служб внешних действий, инициативы ЕС «Team Europe» и Центра передового опыта НАТО/StratCom. IFTCCAD должен дополнительно уделять приоритетное внимание механизмам быстрого реагирования на стресс-тестирование и стремиться финансировать исследования с открытым исходным кодом.

Он должен изучить создание лучших практик для нетехнических решений, таких как медиаграмотность, свободная пресса и инициативы гражданского участия, опираясь на заметную работу проекта Центра стратегических и международных исследований «Защита демократических институтов» и Альянса Немецкого фонда Маршалла за обеспечение демократии.

• Технология слежки, которая согласуется с демократическими ценностями.

ИТЦ должен посвятить многоаспектные усилия продвижению технологий наблюдения, поддерживающих демократические ценности. В частности, усилия должны быть сосредоточены на (a) продвижении технологий, обеспечивающих определенную степень защиты частной жизни личности, гражданских прав и свобод и ограничивающих использование

данных, собранных или объединенных таким образом, чтобы обеспечить повторную идентификацию, и (б) противодействии глобальному развертыванию технологий наблюдения, используемых для подрыва демократических ценностей и прав личности.

Для этого потребуются скоординированные стратегии НИОКР, обмена сообщениями и оказания помощи в целях развития для поддержки демократических альтернатив технологиям, производимым в Китае.

Стимулирование НИОКР, необходимых для обеспечения альтернатив, потребует координации между государственным и частным секторами или партнерства на международном уровне (см. Критическую область № 2 для потенциальных механизмов).

Потенциальные заинтересованные стороны для такого проекта включают NSF, Национальные исследовательские институты ИИ, DARPA, NIST, различные Центры передового опыта ЕС, исследовательские институты (такие как Лаборатория прикладной физики Университета Джона Хопкинса, Массачусетский технологический институт информатики и ИИ и Стэнфордский институт человекоцентричного ИИ), GPAI и неправительственные организации, такие как OpenMined.

Критическая область № 4 – Изучение путей облегчения обмена данными

• *Цели:*

Устраните правовые и нормативные барьеры на пути международной совместной работы; изучите двусторонние и многосторонние, общие и конкретные подходы к обеспечению совместного использования, объединения и хранения данных в соответствии с конфиденциальностью, безопасностью и другими фундаментальными ценностями, включая жизнеспособность свободного потока данных с Соглашением о доверии.

• Методы реализации скоординированных подходов к обмену данными.

Разработка общих сред обработки данных. Разработка объединенных центров хранения данных, вычислительных сред, облачных и пограничных

вычислительных средств для объединения данных из различных источников для свободного использования дипломированными исследователями. Подобный подход оказался бы особенно полезным для улучшения обмена данными между членами альянса «Пять глаз».

Соглашение об основах документирования, маркировки, архивирования и организации данных в международных организациях. Соглашения о данных между членами альянсов (таких как НАТО) или других международных организаций облегчили бы поддержку совместных усилий в области НИОКР; например, текущие усилия Организации экономического сотрудничества и развития (ОЭСР) Обсерватория политики ИИ и Глобальное партнерство по искусственному интеллекту (GPAI).

Соглашения об обмене конкретными наборами данных с определенными иностранными партнерами. Более узкое по охвату, чем вышеупомянутые два подхода, соглашение такого рода позволило бы исследователям из разных стран получить доступ к одним и тем же наборам данных для своих соответствующих проектов. Например, в контексте COVID-19 и здравоохранения60 странам необходимо будет решать вопросы маркировки данных, хранения данных, анонимизации данных, безопасности данных и другие вопросы на совместной основе или в рамках пилотного проекта.

Этот тип усилий может также включать совместные проекты с союзниками по анонимизации высокоэффективных наборов данных для конкретных исследований или инициатив, таких как наборы данных Национальных институтов здравоохранения и наборы данных, поддерживаемые для различных целей Министерством здравоохранения, Агентством США по международному развитию (USAID), Управлением по контролю за продуктами и лекарствами США, DARPA, IARPA и Аналитическим центром Государственного департамента.

Дипломатические усилия необходимы для разрешения разногласий по поводу того, что представляет собой анонимизированные данные, согласие и вопросы, представляющие общественный интерес.

Специальные механизмы обмена данными на двусторонней или многосторонней основе. ЭТП должен изучить готовность стратегических союзников и партнеров участвовать в целевых, недоговорных механизмах обмена данными. Механизмы «песочницы инноваций» могут быть разработаны для облегчения конкретных задач во всех областях — безопасности, здравоохранения, дезинформации, устойчивости окружающей среды и т. д.

Многостороннее соглашение об обмене данными, основанное на доверии. ЕТС должен возглавить усилия по созданию формального, потенциально основанного на договорах подхода к обмену данными, объединению и хранению данных с правительствами-единомышленниками по образцу концепции свободного потока данных с доверием (DFFT), представленной Японией на саммите G20 в июне 2019 года. DFT позволит осуществлять свободный поток данных между уполномоченными сторонами при соблюдении определенных стандартов, включая защиту интеллектуальной собственности (ИС), неприкосновенность частной жизни и кибербезопасность. Европейская комиссия одобрила концепцию DFT в декабре 2020 года.

Общий DFT потребует значительного рассмотрения вопросов защиты данных, защиты ИС, защиты конфиденциальности и торговых вопросов как для внутренних, так и для иностранных партнеров Соединенных Штатов.

С другой стороны, конкретный ДФФТ, ориентированный на свободный поток данных для конкретных целей — таких, как содействие усилиям по реагированию на пандемию, — будет иметь больше шансов на успех и может стать моделью для целевых механизмов обмена данными в других областях, представляющих общий интерес.

Разработка защищенной инфраструктуры исследовательских ресурсов ИИ. Безопасная облачная инфраструктура обеспечит исследователям из стран-партнеров и союзников доступ к вычислительным ресурсам, разнообразным наборам данных и контролируемым средам для тестирования, например, методов мл, сохраняющих конфиденциальность. Участвующие правительства-единомышленники согласятся и будут соблюдать общие технические

стандарты и нормы, а также основанные на риске рамки, обеспечивающие конфиденциальность, безопасность, надежность, уважение верховенства права и другие соответствующие параметры.

Такая инфраструктура могла бы быть развита на двусторонней или многосторонней основе и могла бы стать приоритетной задачей предлагаемой Комиссией MAIRI. Научно-исследовательские и академические учреждения могли бы поддержать усилия MAIRI с соответствующей технической и имплементационной помощью, в то время как Рабочая группа GPAI по управлению данными могла бы поддержать разработку и использование передовых инженерных практик.

Критическая область № 5 – Продвижение и защита инноваций

• *Цели:*

Разработка союзнической стратегии согласования и развития нормативно - правовых режимов в областях, имеющих решающее значение для стимулирования внутренних и международных инноваций. Эти области включают экспортный контроль, скрининг инвестиций, обеспечение цепочки поставок, инвестиции в новые технологии, торговую политику, ИС, передачу технологий и защиту научных исследований.

Достижение такой стратегии потребует комплексного подхода союзников и партнеров, задействования всего нашего технологического инструментария, модернизации возможностей и, при необходимости, разработки новых для противодействия угрозам. Эти усилия потребуют скоординированного стратегического плана координации для повышения осведомленности общественности союзников по таким вопросам, как риски передачи технологий.

• Экспортный контроль и проверка инвестиций

ЕТЦ следует изучить скоординированные подходы к экспортному контролю и проверке инвестиций. Сотрудничество в этих областях имеет решающее значение для обеспечения того, чтобы страны-единомышленники

имели полномочия в одностороннем порядке вводить экспортный контроль и блокировать хищнические инвестиции, представляющие угрозу национальной и международной безопасности.

Комиссия рекомендует Соединенным Штатам совместно с союзниками и партнерами провести правовые реформы с целью a) осуществления скоординированного подхода к экспортному контролю, связанному с ИИ, и b) совершенствования процедур проверки инвестиций и обеспечения их соблюдения.

Комиссия также рекомендовала в рамках Плана действий главы, чтобы Соединенные Штаты взаимодействовали с союзниками и партнерами для согласования руководящих принципов политики в отношении экспорта в рамках Международной инициативы цифровой демократии (IDDI) для продвижения технологий, которые согласуются с общими ценностями и поддерживают свободные и открытые общества.

Как подробно описано, приоритеты экспортного контроля должны включать целевые компоненты высокотехнологичного полупроводникового производственного оборудования (МСП), необходимые для производства чипов на узле 16 нм и ниже. Кроме того, государствам следует изучить вопрос о внедрении целенаправленного контроля за конечным использованием и конечными пользователями конкретных высококачественных специализированных чипов искусственного интеллекта для предотвращения их использования при нарушениях прав человека.

Следует рассмотреть вопрос о соответствующих экономических стимулах для поддержки согласования мер экспортного контроля и проверки инвестиций.

ИТЦ также должен осуществлять активное сотрудничество в области мониторинга иностранных научно—технических и инвестиционных потоков-включая разведывательные данные с открытым исходным кодом—для использования показателей раннего предупреждения, связанных со стратегическими рисками приобретения. Кроме того, партнеры ЕТС должны

делиться передовым опытом для мониторинга небольших транзакций, которые пытаются обойти существующие средства контроля.

• Обеспечение Цепочки Поставок

Лидерство США и их союзников и партнеров в новых технологиях зависит от компонентов, поставляемых стратегическими конкурентами или регионами со значительным геополитическим риском.

Полупроводниковая промышленность является ярким примером отрасли, которая имеет решающее значение для безопасности США и союзников, но которая в значительной степени сосредоточена в определенных географических регионах и поэтому подвержена шокам цепочки поставок, особенно в случае кризиса.

ИТЦ должен провести оценку цепочки поставок и вынести рекомендации по комплексным многосторонним подходам к координации важнейших технологических компонентов для укрепления международной безопасности при одновременном снижении коллективной зависимости от стратегических конкурентов.

ИТЦ также должен разработать стратегический план финансирования ключевых технологий и материалов следующего поколения, подходов и возможностей прототипирования в масштабах открытия, производства и применения.

• Инвестиции в Новые технологии

Точно так же инвестиции в новые технологии требуют скоординированных действий. 5G представляет собой тестовый пример для решения проблем международной и многосторонней координации. Соединенные Штаты и партнеры сотрудничают в разработке альтернатив китайской инфраструктуре 5G на многосторонней и двусторонней основе.

Комиссия предложила рекомендации относительно шагов по содействию внутреннему развитию технологии 5G в своих Рекомендациях за первый квартал и настоятельно призвала Соединенные Штаты продолжать тесно сотрудничать с ключевыми союзниками и партнерами как по конструктивным

техническим решениям 5G, так и по обеспечению безопасности глобальных сетей 5G. В главе 16 настоящего доклада подробно описываются шаги по содействию отечественному развитию биотехнологий, 5G, квантовых вычислений, автономии и робототехники, передового производства и энергетических систем, подробно описываются шаги по развитию отечественных инноваций в области исследований и производства микроэлектроники. Соединенные Штаты могут привлечь ключевых союзников и партнеров по этим технологиям.

ЭТП может служить форумом для скоординированного изучения этих вопросов.

• Торговая политика

Торговая политика является ключевым рычагом для Соединенных Штатов и иностранных правительств по содействию созданию инновационной среды. ЕТЦ должна рассмотреть скоординированные подходы к торговой политике в целях дальнейшего развития инноваций и укрепления национальной и международной безопасности.

• Интеллектуальная Собственность

Права и режимы ИС имеют решающее значение для инноваций в области ИИ и новых технологий. ИТЦ следует изучить скоординированные подходы к ИС, которые могли бы послужить основой для совместной повестки дня с обсуждением Всемирной организацией интеллектуальной собственности (ВОИС) вопросов ИИ и интеллектуальной собственности, ИС573 и форумами с более широкими мандатами.

Координация помощи странам в разработке сильных и согласованных режимов ИС. ИТЦ может помочь Соединенным Штатам и партнерам в определении приоритетов помощи странам в совершенствовании их режимов ИС, чтобы способствовать инновациям и одновременно сдерживать кражу ИС. Более целенаправленный подход с помощью IP5 и IPAD может оказаться более эффективным по масштабу и может помочь гармонизировать усилия по укреплению ИС в отношении идентифицируемых международных проблем.

Соединенным Штатам следует взаимодействовать с ключевыми союзниками и партнерами для согласования критических аспектов ИС, включая право на получение патентов на ИИ и связанные с ним технологии, противодействие китайскому нарративу о победе в инновационном конкурсе, препятствия для международного сотрудничества в области контрактной экосистемы ИС, защиту данных ИС и чрезмерное декларирование «стандартных основных» патентов и другие усилия стран по использованию процессов установления стандартов и лицензирования.

Это один из 10 важнейших аспектов ИС, которые Комиссия предлагает направлять усилия США по реформированию политики в области ИС и созданию новых режимов ИС для ИИ и критических новых технологий в целях защиты и поощрения национальной безопасности, инноваций и технологической конкурентоспособности.75

Скоординированные усилия по пресечению кражи ИС и противодействию кибершпионажу. Кража ИС остается глобальной проблемой. С целью защиты экономической жизнеспособности инноваций в области ИИ и новых технологий ИТЦ должна определить методы укрепления международной базы для борьбы с экспортом контрафактных товаров, кражей технологий ИС, принудительной передачей технологий иностранных инноваций и кибершпионажем.

• Исследования и киберзащита

Содействие многосторонним ответным мерам на обеспечение целостности и безопасности исследований. Как предложила Комиссия, Соединенным Штатам следует координировать действия с союзниками и партнерами в разработке многосторонних ответных мер на вызовы целостности и безопасности исследований, создаваемые связанными с НОАК лицами и организациями, и поощрять приверженность открытым фундаментальным исследованиям.

Информационно-координационный центр по вопросам безопасности исследований между государственным и частным секторами, обеспечивающий

обмен информацией из открытых источников, оценки на основе данных, ресурсы поддержки принятия решений, а также образовательные и учебные ресурсы, мог бы укрепить эти усилия.

Содействие многосторонним усилиям по смягчению распространяющихся кибер-уязвимостей и разработке средств защиты от кибератак с использованием искусственного интеллекта. Как предложила Комиссия, Соединенные Штаты должны подготовиться к киберконфликту с использованием искусственного интеллекта. Соединенным Штатам следует изучить возможность координации и совместных усилий с ключевыми союзниками и партнерами.

Критическая область № 6 – Развитие талантов, связанных с искусственным интеллектом

• Цели:

Совместные усилия по обеспечению обмена талантами между правительством, военными, академическими кругами и частным сектором и решению проблем, связанных с иммиграционными и визовыми ограничениями; разработка совместных программ обучения искусственному интеллекту и цифровым технологиям и развития рабочей силы.

• Методы содействия развитию талантов во всем мире. ИТЦ должен изучить методы достижения целей, включая следующие:

Создание новых моделей для международного обмена талантами. Международные обмены талантами являются мощными инструментами для дальнейшего выравнивания ИИ, перекрестного опыления идей и создания навыков и возможностей, связанных с ИИ. При разработке новых подходов к обмену талантами ИТЦ следует учитывать:

Обмен военными офицерами для улучшения развертывания и взаимодействия ИИ, в том числе между НАТО, СОКОМ, Минобороны, министерствами обороны иностранных государств и военными;

Аналогичная подготовка и обмены, необходимые для дипломатов США и союзников, и экспертов в области развития;

Государственные обмены экспертами в области искусственного интеллекта для оказания помощи в создании технических и этических экспертных знаний; обмены в интересах отраслевых многосторонних и многосторонних усилий, таких как SDOS, GPAI, OECD, и влияние на пути, избранные партнерами;

Обмен талантами и прикомандирование в промышленность и академию (как международные обмены талантами между промышленностью и академией, так и государственные обмены талантами между промышленностью и академией); и

Использование исследовательских центров, таких как предлагаемый MAIRI, для обеспечения трансграничного сотрудничества и обмена талантами.

Координация программ развития обучения ИИ и обмен передовым опытом в области государственного обучения и более широких образовательных программ ИИ (в том числе в средних школах и университетах, включая преподавание компьютерных наук и разработку учебных программ).

ИТЦ должен изучить методы координации действий стран-партнеров, не входящих в ЕС, по теме «Искусственный интеллект и аналитика» в Плане цифрового образования ЕС.

Критическая область № 7 – Международная инициатива цифровой демократии

• В главе плана действий подробно излагаются рекомендации Комиссии по координации иностранной помощи, инвестиций и финансирования в рамках Международной инициативы по цифровой демократии.

Благоприятный международный технологический порядок

Ссылки и ресурсы

1. См. Промежуточный отчет и рекомендации за третий квартал, NSCAI at 213 (октябрь 2020 г.), https://www.nscai.gov/previous-reports/.

2. См. Приложение к настоящему отчету, содержащее сокращенную версию ключевых соображений NSCAI по ответственной разработке и

внедрению ИИ. Дополнительные сведения о рекомендациях Комиссии по отстаиванию демократических ценностей см. в разделе «Приведение систем и видов использования в соответствие с американскими ценностями и верховенством закона» в разделе «Ключевые соображения ответственного развития и внедрения искусственного интеллекта: Расширенная версия», NSCAI (2021) (имеется в архиве Комиссии).

3. Ключевые организации по техническим стандартам включают Международную организацию по стандартизации (ИСО), Международную электротехническую комиссию (МЭК), Институт инженеров электротехники и электроники (IEEE), Сектор стандартизации электросвязи Международного союза электросвязи ООН (МСЭ-Т) и Партнерский проект третьего поколения (3GPP). См. Промежуточный отчет и рекомендации за третий квартал, NSCAI at 205 (октябрь 2020 г.), https://www.nscai.gov/previous-reports/.

4. См. Рекомендации второго квартала, NSCAI at 89 (июль 2020 г.), https://www.nscai.gov/previous-reports/.

5. См. Промежуточный отчет и рекомендации за третий квартал, NSCAI at 213 (октябрь 2020 г.), https://www.nscai.gov/previous-reports/. 6 Id.

7. Комиссия рекомендует NIST предоставить набор стандартов, показателей эффективности и инструментов для обеспечения квалифицированного доверия к моделям ИИ, данным, учебным средам и прогнозируемым результатам. План действий также рекомендует, чтобы NIST обеспечивал руководство по мере развития науки о тестировании всех ответственных атрибутов ИИ.

8. Дженни Теннисон, Введение в работу Глобального партнерства по управлению данными ИИ, Обсерватория политики ИИ ОЭСР (21 августа 2020 года), https://oecd.ai/wonk/an-introduction-to-the-global-partnership-on-ais-work-on-data-governance.

9. ОЭСР возглавляет международное сообщество в своей работе над нормами ИИ и разработкой политики. Майские принципы искусственного интеллекта 2019 года стали первым многосторонним сводом принципов,

принятых правительствами. Запущенная в феврале 2020 года Обсерватория политики ИИ ОЭСР облегчает диалог между ее глобальными многосторонними заинтересованными сторонами, обеспечивает основанный на фактических данных анализ по более чем 20 областям политики, способствует принятию Принципов ИИ и поддерживает продвижение и мониторинг надежных систем ИИ, которые приносят пользу обществу. Сеть экспертов по ИИ (ONE AI)-это неофициальная консультативная группа междисциплинарных и многосторонних экспертов из более чем 30 стран, которая обеспечивает политический, технический и деловой экспертный вклад в анализ и рекомендации ОЭСР. ОЭСР также разработала Руководящие принципы по защите частной жизни и Трансграничным потокам персональных данных и работает над принципами доверенного правительственного доступа к данным. См. также OECD AI Policy Observatory, OECD.AI (последний доступ 5 января 2021 года), https://oecd.ai/; OECD Privacy Guidelines, OECD (последний доступ к янв. 4, 2020), http://www.oecd.org/digital/ieconomy/privacy-guidelines.htm.

10. См. Технический глоссарий терминов ИИ в приложении к настоящему отчету для определения методов гомоморфного шифрования и дифференциальной конфиденциальности. Совместные исследования в этой области могли бы опираться на перспективные примеры использования НИОКР, включая программу DARPA Brandeis и программу IARPA HECTOR. См. Brandeis, DARPA (последний доступ 18 сентября 2020 года), https://www.darpa.mil/program/brandeis; Гомоморфные методы шифрования вычислений с уменьшением накладных расходов (HECTOR), IARPA (последний доступ 18 сентября 2020 г.), https://www.iarpa.gov/index.php/research-programs/hector; см. Приложение к настоящему отчету, содержащее сокращенную версию ключевых соображений NSCAI по ответственной разработке и внедрению ИИ. Дополнительные сведения о рекомендации Комиссии в отношении будущих НИОКР, необходимых для расширения возможностей сохранения и обеспечения американских ценностей и верховенства права, см. в разделе «Приведение

систем и видов использования в соответствие с американскими ценностями и верховенством права» в разделе «Ключевые соображения ответственного развития и внедрения искусственного интеллекта: Расширенная версия», NSCAI (2021) (имеется в архиве Комиссии).

11. См. Рекомендации за первый квартал, NSCAI at 11 (март 2020 г.), https://www.nscai.gov/previous-reports/.

12. См. Приложение к настоящему отчету, содержащее сокращенную версию ключевых соображений NSCAI по ответственной разработке и внедрению ИИ. Дополнительные сведения о рекомендации Комиссии в отношении будущих НИОКР, необходимых для расширения возможностей TEVV, см. в разделе «Производительность системы» в разделе «Ключевые соображения для ответственной разработки и внедрения искусственного интеллекта: Расширенная версия», NSCAI (2021) (имеется в архиве Комиссии). НИОКР TEVV включает в себя комплексное системное тестирование для улучшения понимания и уверенности в эмерджентной производительности составленных систем ИИ, а также совершенствования методов понимания, прогнозирования и управления системами систем, чтобы избежать негативных результатов, возникающих в результате взаимодействия систем. Кроме того, НИОКР в мультиагентном сценарии продвинут понимание взаимодействующих систем ИИ, включая применение теории игр к разнообразным и сложным сценариям и взаимодействиям между когортами, состоящими из смеси людей и технологий ИИ. См. также Рекомендации за первый квартал, NSCAI at 11 (март 2020 г.), https://www.nscai.gov/previous-reports/.

13. Комиссия ранее рекомендовала Соединенным Штатам выделять больше ресурсов на моделирование ИИ, имитационное моделирование и проектирование. См. Рекомендации за первый квартал, NSCAI, 6-13 (март 2020 г.), https://www.nscai.gov/previous-reports/.

14. См. Технический глоссарий терминов ИИ в Приложении к настоящему отчету для определения однократного (или несколькихкратного) обучения.

15. См. Рекомендации за первый квартал, NSCAI at 11 (март 2020 г.), https://www.nscai.gov/previous-reports/.

16. См. Приложение к настоящему отчету, содержащее сокращенную версию ключевых соображений NSCAI по ответственной разработке и внедрению ИИ. Дополнительные сведения о рекомендации Комиссии в отношении будущих НИОКР, необходимых для развития возможностей обеспечения безопасности и надежности ИИ, см. в разделе «Инженерные практики» в разделе «Ключевые соображения ответственной разработки и внедрения искусственного интеллекта: Расширенная версия», NSCAI (2021) (имеется в архиве Комиссии). См. также Рекомендации за первый квартал, NSCAI at 11 (март 2020 г.), https://www.nscai.gov/previous-reports/.

17. См. Приложение к настоящему отчету, содержащее сокращенную версию ключевых соображений NSCAI по ответственной разработке и внедрению ИИ. Дополнительные сведения о рекомендациях Комиссии по тестированию взаимодействия машина-машина/мультиагент , а также о международном сотрудничестве и сотрудничестве, необходимых для согласования того, как тестировать и проверять надежность и производительность систем искусственного интеллекта в соответствии с общими ценностями, см. в разделе «Производительность системы» в разделе «Ключевые соображения для ответственной разработки и внедрения искусственного интеллекта: Расширенная версия», NSCAI (2021) (в файле Комиссии).

18. Подробнее о потенциальных приоритетных областях исследований ИИ см. Главу 11 настоящего доклада и связанный с ней План действий.

19. См. Рабочую группу по ядерной критической безопасности (WPNCS), Агентство ОЭСР по ядерной энергии, https://www.oecd-nea.org/science/wpncs/; Международное сотрудничество в области оценки ядерных данных:

Расширенное резюме Пилотного проекта Совместной Международной библиотечной организации по оценке (CIELO), NEA No. 7489, OECD Nuclear Energy Agency (2019), https://www.oecd-nea.org/science/wpec/documents/volume40.pdf.

20. GEOTHERMICA объединяет финансовые ресурсы и опыт в области исследований и инноваций в области геотермальной энергетики из 16 стран и их регионов. Она «запускает совместные проекты, демонстрирующие и подтверждающие новые концепции внедрения геотермальной энергии в энергетическую систему и определяющие пути к коммерческому крупномасштабному внедрению.» Одна из трех основных областей включает в себя «интеллектуальную интеграцию в энергетическую систему и операции.» Некоторые из проектов имеют аспекты больших данных и интеллектуальных систем, такие как Французский национальный проект через проект GEOTHERMICA HEATSTORE. Партнеры GEOTHERMICA, такие как американская национальная лаборатория Лоуренса Ливермора, обладают опытом в области мл. См. О GEOTHERMICA, GEOTHERMICA (последний доступ 18 сентября 2020 года), http://www.geothermica.eu/about-geothermica/; Французский национальный проект, HEATSTORE (последний доступ 18 сентября 2020 года), https://www.heatstore.eu/national-project-france.html; Американские партнеры, GEOTHERMICA (последний доступ 18 сентября 2020 г.), http://www.geothermica.eu/matchmaking/united-states/.

21. Членами партнерства являются Соединенные Штаты, а также Австралия, Германия, Китай, Япония, Россия, Австрия, Коста-Рика, Исландия, Республика Корея, Южная Африка, Бразилия, Индия, Нидерланды, Канада, Франция, Италия и Норвегия. См. Международное партнерство по водороду и топливным элементам в экономике, Министерство энергетики США (последний доступ 18 сентября 2020 года), https://www.energy.gov/eere/fuelcells/international-partnership-hydrogen-and-fuel-cells-economy; Международное партнерство по водороду и топливным

элементам в экономике, IPHE (последний доступ 18 сентября 2020 г.), https://www.iphe.net/.

22. См. Промежуточный отчет и рекомендации за третий квартал, NSCAI at 153 (октябрь 2020 г.), https://www.nscai.gov/previous-reports/.

23. Глава 16 и связанный с ней План действий рекомендуют Соединенным Штатам развивать глобальное сотрудничество в области интеллектуального мониторинга заболеваний.

24. Jason Matheny, et al., The Role of AI Technology in Pandemic Response and Readiness: Recommended Investments and Initiatives, NSCAI (25 июня 2020 г.), https://www.nscai.gov/white-papers/covid-19-white-papers/.

25. См.Главу 11 настоящего доклада и связанный с ним План действий, в котором содержится рекомендация Соединенным Штатам взять на себя некоторые из самых больших проблем человечества.

26. Nano EHS Cord, US-EU Nanotechnology Communities of Research (Cars) (последний доступ 18 сентября 2020 года), https://us-eu.org/communities-of-research/.

27. См., например, Jeff Mason и др., Обзор клинических применений искусственного интеллекта, Канадское агентство по лекарственным средствам и технологиям в здравоохранении (сентябрь 2018 г.), https://www.cadth.ca/sites/default/files/pdf/eh0070_overview_clinical_applications_of_AI.pdf.

28. Feed The Future (последний доступ 3 февраля 2021 года), https://www.feedthefuture.gov/.

29. Автоматизация и искусственный интеллект в сельском хозяйстве: Будущее поддержания продовольственной безопасности и устойчивой интенсификации, Границы (последний доступ 3 февраля 2021 года), https://www.frontiersin.org/research-topics/15206/automation-and-artificial-intelligence-in-agriculture-the-future-of-maintaining-food-security-and-su.

30. Всемирный экономический форум отметил, что 160 миллионов человек в год подвергаются риску стихийных бедствий, и видит большую

пользу в ИИ от «сокращения времени оценки ущерба для мониторинга социальных сетей для более быстрой и эффективной доставки помощи» и «оттачивания решений сотрудников по оказанию помощи на передовой».» Эшли ван Гетерен и др., Стихийные бедствия становятся все более частыми и свирепыми. Вот как ИИ может прийти на помощь, Всемирный экономический форум (14 января 2020 года), https://www.weforum.org/agenda/2020/01/natural-disasters-resilience-relief-artificial-intelligence-ai-mckinsey/.

31. Дэвид Вергун, DOD Partners With Agencies to Use AI for Disaster Relief, Humanitarian Relief, DOD News (20 Августа 2020), https://www.defense.gov/Explore/News/Article/Article/2319945/dod-partners-with-agencies-to-use-ai-for-disaster-humanitarian-relief/.

32. Прашант Парамешваран, Что входит в Новое американо-Сингапурское оборонное партнерство по искусственному интеллекту?, The Diplomat (1 июля 2019 года), https://thediplomat.com/2019/07/whats-in-the-new-us-singapore-artificial-intelligence-defense-partnership/.

33. См. Обсуждение в главе 11 и связанный с ним План действий по использованию ИИ для решения некоторых из самых больших проблем человечества.

34. Об астероидах см. Deep Asteroid, NASA (27 мая 2016 г.), https://open.nasa.gov/innovation-space/deep-asteroid/.

35. ИИ бросил вызов предотвратить столкновения в космосе, Европейское космическое агентство (9 октября 2019 года), https://www.esa.int/Enabling_Support/Space_Engineering_Technology/AI_challenged_to_stave_off_collisions_in_space; Анжелика Мари, Правительство Великобритании Ищет инновации для борьбы с космическим мусором, Computer Weekly (28 мая 2020 года), https://www.computerweekly.com/news/252483762/UK-government-seeks-innovations-to-tackle-space-debris.

36. Эндрю Майерс, Стэнфорд Разрабатывает навигационную систему искусственного интеллекта для будущего спутникового ‘Эвакуатора’, Stanford

News (1 февраля 2019 года), https://news.stanford.edu/2019/02/01/stanford-spurs-ai-navigation-space-rendezvous-software/.

37. Лесли Д'Монте, Чандраян-2 Прагьян Показывает, как ИИ помогает освоению космоса, Монетный двор (6 сентября 2019 года), https://www.livemint.com/technology/tech-news/chandrayaan-2-pragyan-shows-how-ai-is-helping-space-exploration-1567764065716.html.

38. Майк Уолл, Новый, Эмоционально Интеллектуальный робот САЙМОН 2 Направляется на Космическую станцию, Space.com (5 декабря 2019 года), https://www.space.com/cimon-2-artificial-intelligence-robot-space-station.html.

39. ЕС намерен создать Центры передового опыта и Центры цифровых инноваций, ориентированные на искусственный интеллект. ICEMAI сотрудничает с Консультативным советом правительства Канады по искусственному интеллекту, Форумом IA Quebec и Международной обсерваторией по социальным последствиям искусственного интеллекта и цифровых технологий и получает поддержку правительств Канады и Квебека с финансированием до 15 миллионов долларов в течение пяти лет. INRIA была запущена в феврале 2020 года и имеет контракт с правительством Франции, чтобы сосредоточиться на «ускорении развития научно-технического лидерства Франции в рамках общеевропейского подхода», включая приоритетность искусственного интеллекта и других цифровых технологий для решения социальных проблем, строительство европейских исследовательских и инновационных пространств, укрепление технологической промышленной базы, укрепление государственной политики и развитие ведущих исследовательских университетов. См. Коммуникационный искусственный интеллект для Европы, Европейская комиссия (25 апреля 2018 г.), https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe; Глобальное партнерство по искусственному интеллекту Официально запущено, Монреальский международный форум (15 июня 2020 года), https://www.montrealinternational.com/en/news/the-global-partnership-on-

artificial-intelligence-officially-launched/; INRIA: For Scientific, Technical and Industrial Leadership in Digital Technology, Government of France (Feb. 24, 2020), https://www.gouvernement.fr/en/inria-for-scientific-technological-and-industrial-leadership-in-digital-technology.

40. См. План реализации Главы 15: Благоприятный международный цифровой порядок.

41. ИИ Для решения глобальных проблем, XPRIZE (последний доступ 18 сентября 2020 года), https://www.xprize.org/prizes/artificial-intelligence.

42. Melissa Flagg & Paul Harris, System Re-engineering: A New Policy Framework for the American R&D System in a Changed World, Center for Security and Emerging Technology (сентябрь 2020), https://cset.georgetown.edu/research/system-re-engineering/.

43. Национальные исследовательские институты искусственного интеллекта-это совместные правительственные усилия Национального научного фонда (NSF), Национального института продовольствия и сельского хозяйства Министерства сельского хозяйства США (USDA), Научно-технического управления Министерства внутренней безопасности США (DHS) и Федерального управления автомобильных дорог Министерства транспорта США (DOT). См. National Artificial Intelligence (AI) Research Institutions, NSF (последний доступ 18 сентября 2020 г.), https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=505686.

44. См. Главу 8 настоящего доклада и связанный с ним План действий для его рекомендации Конгрессу разрешить NIST спонсировать Университетский исследовательский центр (UARC), Финансируемый из Федерального бюджета научно-исследовательский центр (FFRDC) и/или лабораторию для проведения независимых сторонних испытаний.

45. Проект AI4EU был основан Европейской комиссией в рамках программы H2020 для создания первой европейской платформы и экосистемы AI On-Demand. Платформа предназначена для поддержки экосистемы ИИ и обеспечивает форум для обмена ресурсами ИИ из европейских проектов. См. О

проекте AI4EU (последний доступ 18 сентября 2020 года), https://www.ai4eu.eu/about-project.

46. ИИ для человечества, Милан (последний доступ 18 сентября 2020 года), https://mila.квебек/ia-dans-la-societe/.

47. Искусственный интеллект для добра и для всех, Amii (последний доступ 18 сентября 2020 года), https://www.amii.ca/.

48. См. Pan-Canadian AI Strategy, CIFAR (последний доступ 4 февраля 2021 года), https://www.cifar.ca/ai; О нас, Vector Institute for Artificial Intelligence (последний доступ 18 сентября 2020 года), https://vectorinstitute.ai/about/.

49. См. Стэнфордский институт человекоцентричного искусственного интеллекта (последний доступ 18 сентября 2020 года), https://hai.stanford.edu/welcome.

50. США имеют прочные исследовательские связи с Израилем через Бинациональный научный фонд (BSF) и Бинациональный фонд промышленных исследований и разработок (BIRD). См. О BSF, Американо-Израильском бинациональном научном фонде (последний доступ 3 февраля 2021 года), https://www.bsf.org.il/about/; Что такое BIRD? Американо-израильские бинациональные промышленные исследования и разработки (последний доступ 3 февраля 2021 года), https://www.birdf.com/what-is-bird/. Индо-США Научно-технический форум (IUSSTF) курирует Американо-Индийский научно - технический эндаумент-фонд (USISTEF), который поддерживает и поощряет совместные прикладные НИОКР. О Фонде, Индо-Американский научно-технический форум (последний доступ 3 февраля 2021 года), https://www.iusstf.org/usistef/us-india-science-technology.

51. См. Совместное заявление об искусственном интеллекте и правах человека, Freedom Online Coalition (последнее обращение 5 января 2021 года), https://freedomonlinecoalition.com/wp-content/uploads/2020/11/FOC-Joint-Statement-on-ArtificiaI-Intelligence-and-Human-Rights.pdf.

52. NDAA FY 2021 создала Фонд открытых технологий в качестве раздела 309A Закона США о международном вещании 1994 года. Pub. L. 116-

283, sec. 1299P, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021). С тех пор Конгресс выделил фонду 20 миллионов долларов. См. Совместное пояснительное заявление, Отдел К– Закон об ассигнованиях Государственного департамента, иностранных операций и связанных с ними программ, 2021 год, 23 (2021), https://www.appropriations.senate.gov/imo/media/doc/Division%20K%20-%20SFOPS%20Statement%20FY21.pdf (введено в действие в Пуб. Л. 116-260, Сводный закон об ассигнованиях, 2021). Отдел свободы Интернета, бизнеса и прав человека Государственного департамента (IFBHR) в рамках DRL возглавляет политику правительства США и взаимодействие по защите прав человека в Интернете. См. «Свобода Интернета: Информационный бюллетень», Государственный департамент США (17 ноября 2017 г.), https://2017-2021.state.gov/internet-freedom/index.html. IFBHR работает в правительстве США, с демократическими странами, с гражданским обществом и с коалицией Freedom Online. Программа IFBHR включает в себя финансирование развития технологий одноранговых коммуникаций, побеждающих цензуру. См. Internet Freedom: Advancing and Promoting Peer-to-Peer Communications Technologies, Государственный департамент США (13 февраля 2020 г.), https://2017-2021.state.gov/internet-freedom-advancing-and-promoting-peer-to-peer-communications-technologies/index.html.

53. Исаак Бен-Исраэль и др., К регулированию систем искусственного интеллекта: Глобальные перспективы развития Правовой базы систем искусственного интеллекта (ИИ) На основе Стандартов Совета Европы по правам человека, демократии и верховенству права, Секретариат КАХАЙ (декабрь 2020 г.), https://rm.coe.int/prems-107320-gbr-2018-compli-cahai-couv-texte-a4-bat-web/1680a0c17a.

54. См. План действий в главе 14. См. также Руководство по реализации Руководящих принципов ООН для транзакций, связанных с конечными пользователями иностранных правительств для Продуктов или услуг с возможностями наблюдения, Государственный департамент США (последний

доступ 4 января 2021 года), https://www.state.gov/wp-content/uploads/2020/10/DRL-Industry-Guidance-Project-FINAL-1-pager-508-1.pdf.

55. Более подробную информацию об этом предложении см. в главе 1 «План действий в отношении вредоносной информации».

56. О Глобальном Интернет-форуме по борьбе с терроризмом (последний доступ 5 января 2021 года), https://www.gifct.org/about/.

57. Гражданское общество на Тайване отреагировало на угрозу со стороны дезинформации несколькими способами, включая демонстрацию за пределами скомпрометированных медиа-фирм, просвещение пожилых граждан о том, как они могут подвергаться дезинформации, и создание надежных групп проверки фактов, таких как Тайваньский центр проверки фактов, MyGoPen, Cofacts и Rum Toast. Эти группы работали как с правительством, так и с платформами социальных сетей, чтобы не только выявлять и удалять дезинформацию, но и криминалистически отслеживать дезинформацию до источников в Китае. См. Одри Тан о цифровой демократии Тайваня, COVID-19 и борьбе с дезинформацией, Центр Стимсона (18 марта 2020 года), https://www.stimson.org/2020/interview-with-taiwan-digital-minister-audrey-tang/.

58. Подробнее о демократическом использовании технологий слежки читайте в главе 8 настоящего доклада «Защита демократических ценностей: Неприкосновенность частной жизни, гражданские свободы и гражданские права при использовании ИИ в интересах национальной безопасности».

59. Кара Фредерик, The Razor's Edge: Liberalizing the Digital Surveillance Ecosystem, CNAS (3 сентября 2020 г.), https://www.cnas.org/publications/reports/the-razors-edge-liberalizing-the-digital-surveillance-ecosystem.

60. См. Усилия OpenMined по борьбе с пандемией коронавируса: COVID Alert App, Private Set Interaction, A Differential Privacy Wrapper and Private Identity, OpenMined (1 апреля 2020 года), https://blog.openmined.org/openmineds-efforts-for-the-coronavirus-pandemic/.

61. США и Европа должны согласовать общее определение анонимизированных данных, включающее более четкое понимание того, что представляет собой «согласие» и «вопросы, представляющие общественный интерес.»

62. Выступление Генерального секретаря ОЭСР Анхеля Гуррии на саммите лидеров G20 2019 года–Digital (AI, data governance, digital trade, taxation) (28 июня 2019 года), https://www.oecd.org/g20/summits/osaka/2019-g20-leaders-summit-digital-osaka-june-2019.htm.

63. Новая повестка дня ЕС-США по глобальным изменениям, Европейская комиссия (2 декабря 2020 г.), https://ec.europa.eu/info/sites/info/files/joint-communication-eu-us-agenda_en.pdf.

64. Можно было бы использовать ключевые соображения Комиссии и существующие международные принципы, такие как Принципы ОЭСР по ИИ, Руководящие принципы ОЭСР по защите частной жизни и трансграничным потокам персональных данных, Рекомендация ОЭСР по цифровой безопасности критических видов деятельности, предстоящие Принципы ОЭСР по доверенному правительственному доступу к данным и другие.

65. См. Главу 14 настоящего доклада и связанный с ней План действий для получения дополнительной информации о рекомендациях Комиссии относительно согласования режимов экспортного контроля союзников и скрининга инвестиций. В правительстве США уже начали такую работу Государственные департаменты и министерства торговли, занимающиеся экспортным контролем, а также Государственные департаменты и Министерство финансов, занимающиеся проверкой инвестиций.

66. См. План действий в другой главе

67. См. Рекомендации второго квартала, NSCAI at 63-67 (июль 2020 г.), https://www.nscai.gov/previous-reports/. В частности, Соединенным Штатам, Нидерландам и Японии следует координировать экспортный контроль за инструментами для иммерсионной литографии с экстремальным ультрафиолетовым излучением и АРФ, поскольку это ограничит возможности

Китая и других конкурентов по разработке высокотехнологичной микроэлектроники, которая становится все более важной для ИИ. Дополнительные сведения о рекомендациях Комиссии в отношении экспортного контроля в отношении МСП см. в главе 14 настоящего доклада.

68. Дополнительные сведения и рекомендации по цепочке поставок микроэлектроники см. в главе 13 настоящего отчета.

69. См. главы 3 и 14 настоящего доклада.

70. См. Рекомендации второго квартала, NSCAI at 48 (июль 2020 г.), https://www.nscai.gov/previous-reports; Andrew Imbrie et al., Agile Alliances: How the United States and Its Alliances Can Deliver a Democratic Way of AI, Center for Security and Emerging Technology at 16-17 (Feb. 2020), https://cset.georgetown.edu/research/agile-alliances/; Andrew Imbrie, et al., The Question of Comparative Advantage in Artificial Intelligence: Enduring Strengths and Emerging Challenges for the United States, Center for Security and Emerging Technology at 33 (Jan. 2020), https://cset.georgetown.edu/wp-content/uploads/CSET-The-Question-of-Comparative-Advantage-in-Artificial-Intelligence-1.pdf.

71. Рекомендации за первый квартал, NSCAI at 45 (март 2020 г.), https://www.nscai.gov/previous-reports/.

72. См. главы 13 и 16 настоящего доклада.

73. «IP5» - это название форума пяти крупнейших мировых ведомств ИС, который был создан для повышения эффективности процесса экспертизы патентов во всём мире. См. О сотрудничестве IP5, fiveIPoffices (последний доступ 4 января 2021 года), https://www.fiveipoffices.org/about.

74. См. Главу 12 настоящего доклада и связанный с ней План действий.

Глава 15: Благоприятный Международный Технологический Порядок

Приложение: Коалиция за новые технологии — Примечания

75. См. Главу 12 настоящего доклада и связанный с ней План действий.

76. См. главу 10 настоящего доклада.

77. Этот подход был рекомендован Мелиссой Флэгг и Закари Арнольдом. См. Melissa Flagg & Zachary Arnold, A New Institutional Approach to Research Security in the United States Defending a Diverse R&D Ecosystem, Center for Security and Emerging Technology (Jan. 2021), https://cset.georgetown.edu/research/a-new-institutional-approach-to-research-security-in-the-united-states/.

78. См. Главу 1 и связанный с ней План действий по подготовке к киберконфликту с поддержкой искусственного интеллекта.

Сопутствующие технологии

План действий

Признавая, что лидерство в области искусственного интеллекта (ИИ) опирается на лидерство во всём наборе новых технологий, Соединенные Штаты должны уделять приоритетное внимание исследованиям и разработкам (НИОКР), применению и внедрению не только ИИ, но и технологий, которые обеспечивают его и поддерживаются им. Этот процесс должен основываться на тщательном анализе угроз и возможностей национальной безопасности на стыке ИИ и связанных с ним технологий. Если правительство США не сможет принять более стратегический подход к защите и продвижению интересов США. имея преимущества в этих областях, она рискует поставить под угрозу технологическое лидерство страны, экономическое процветание и национальную безопасность.

В соответствии со своим мандатом рассматривать как ИИ, так и «связанные с ним технологии», Комиссия определяет и предлагает шаги по сохранению лидерства США по всему спектру технологий, которые, по ее мнению, наиболее важны для национальной конкурентоспособности США. Затем Комиссия предлагает конкретные рекомендации о том, как Соединенные Штаты могут активно реагировать на новые угрозы национальной безопасности и возможности, создаваемые, в частности, тремя технологиями:

биотехнологией, квантовыми вычислениями и телекоммуникациями 5G. Наконец, Комиссия расширяет свой анализ, включив в него рекомендации по более широкому набору новых технологий, имеющих решающее значение для национальной конкурентоспособности США.

Технологии, критически важные для национальной конкурентоспособности США

Комиссия определила восемь технологий и связанных с ними платформ, которые являются ключевыми для лидерства США. Две из этих технологий — искусственный интеллект и микроэлектроника—рассматриваются в других разделах настоящего доклада. Остальные шесть — биотехнологии, квантовые вычисления, 5G и передовые сети, автономия и робототехника, современное и аддитивное производство и энергетические системы—рассматриваются ниже. Эти рекомендации основаны на предыдущей работе Комиссии, предусматривая действия, которые правительство США могло бы предпринять для содействия общему развитию США. лидерство и долгосрочная конкурентоспособность в созвездии новых технологий.

Рекомендация: Определить и определить приоритетность технологий, имеющих центральное значение для национальной конкурентоспособности.

На сегодняшний день нет общегосударственного консенсуса в отношении того, какие новые технологии являются наиболее важными для долгосрочной стратегической конкурентоспособности и чье развитие должно быть приоритетным. Несколько правительственных учреждений предприняли независимые попытки определить такой список: Стратегия национальной обороны на 2018 год, список «критических новых технологий», подготовленный Министерством обороны в ответ на раздел 1793 Закона о разрешении национальной обороны на 2019 финансовый год (NDAA), Предварительное уведомление Министерства торговли о предлагаемом нормотворчестве (ANPRM) контроля над некоторыми новыми технологиями на 2018 год, доклад Совета советников Президента по науке и технике под названием «Рекомендации по укреплению американского лидерства в отраслях

будущего с 2020 года», и законопроект, внесенный сенатором Чаком Шумером в 116-й Конгресс с семью двухпартийными соавторами под названием «Закон о бесконечных границах». Кроме того, Белый дом опубликовал Национальную стратегию критических и новых технологий в октябре 2020 года, которая включала список критических и новых технологий. Однако этот документ не объясняет, почему каждая из этих технологий имеет важное значение для национальной конкурентоспособности США, и не содержит конкретных планов внедрения для содействия их развитию и защиты преимуществ США в каждой из них.

Эти списки имеют существенное перекрытие, но нет двух одинаковых списков, и ни один список не является авторитетным. Следовательно, нет общегосударственного консенсуса и, конечно же, национального консенсуса, технологии которого имеют решающее значение для национальной конкурентоспособности США, что затрудняет правительству США управление инвестициями частного сектора, законодателям-определение приоритетов финансирования, а государственным учреждениям-координацию защиты и продвижения технологий. Также нет списка, вокруг которого Белый дом мог бы организовать национальную технологическую стратегию, и нет скоординированного механизма внутри правительства США для поддержки финансирования этих приоритетов в случае провалов рынка и недостаточного финансирования частного сектора.

Действия для Администрации Президента:

• Определить и расставить приоритеты в ключевых новых технологиях, в которых лидерство США необходимо.

Администрация Президента, в консультации с департаментами и ведомствами, должна опубликовать единый авторитетный список технологий и секторов, которые являются ключевыми для общей конкурентоспособности США, а также подробные планы реализации для каждого из них, чтобы обеспечить долгосрочное лидерство США.

В планах внедрения должны быть определены конкретные подкомпоненты каждой технологии, которые являются наиболее важными, ключевые узловые точки, где конкуренты могут быть заблокированы с минимальным воздействием на промышленность США, и где необходимы дополнительные ресурсы. Эти планы должны включать конкретные шаги по развитию отечественной промышленности, обеспечению устойчивости цепочек поставок и защите ключевых технологий от конкурентов. Этот перечень технологий и связанные с ним планы осуществления составят основу Национальной технологической стратегии.

Создание и ведение такого перечня и планов реализации поможет выработать национальный консенсус относительно того, какие отрасли являются наиболее важными в формирующейся технико-экономической конкуренции. Результатом станет важное послание Конгрессу о том, где страна должна расставлять приоритеты и расходовать ресурсы, а также мощный сигнал спроса для промышленности. На рисунке ниже представлены восемь технологий, которые Комиссия рекомендует рассмотреть для включения в этот список.

• Расширить кредитные полномочия Финансовой корпорации развития, включив в них возможности отечественной промышленной базы, поддерживающей ключевые новые технологии.

Президент должен издать Исполнительный указ, расширяющий полномочия по предоставлению займов Американской Международной финансовой корпорации развития (DFC), включив в них возможности национальной промышленной базы, связанные с любой из вышеупомянутых технологий, которые определены Администрацией Президента как ключевые для общей конкурентоспособности США.

В частности, Исполнительный указ должен делегировать DFC полномочия в соответствии с разделом III Закона об оборонном производстве выдавать кредиты, которые «создают, поддерживают, защищают, расширяют или восстанавливают возможности национальной промышленной базы»,

поддерживающие вышеупомянутый перечень технологий, или «устойчивость соответствующих внутренних цепочек поставок». Эта новая власть должна быть бессрочной.

Это действие будет основываться на Исполнительном указе 13922, который расширил аналогичные внутренние кредитные полномочия до DFC, связанные с отраслями, поддерживающими «национальные ответные меры и восстановление после вспышки COVID-19» до 2022 года.

Расширение внутренних полномочий DFC в том, что касается критических технологий, поможет правительству поддержать ключевые платформы и проекты, которые имеют решающее значение для будущей национальной безопасности и экономической конкурентоспособности США, но не имеют достаточного капитала частного сектора.

DFC следует координировать свои действия с Советом по конкурентоспособности технологий, рекомендованным, для определения конкретных платформ, которые больше всего нуждаются в таком финансировании.

Обеспечение лидерства США в области биотехнологий

Сочетание достижений в области искусственного интеллекта и биологии способно изменить мировую экономику в следующем столетии. Прогресс в генетическом секвенировании дал исследователям возможность читать «код жизни».» Учитывая значительный объем данных, ИИ будет иметь важное значение для полного понимания того, как генетический код взаимодействует с биологическими процессами. Наконец, достижения в области синтетической биологии и генетического редактирования дадут исследователям возможность манипулировать этим кодом для выполнения определенных функций. Вместе эти методы позволят осуществить трансформационные прорывы в биологии и послужат основой для большинства будущих научных прорывов, связанных со здоровьем человека, сельским хозяйством и климатологией. Страна, которая лучше всего сможет одновременно использовать обе технологии, будет иметь значительные стратегические преимущества в обозримом будущем,

потенциально став мировым лидером в области фармацевтики, сократив свою зависимость от иностранных цепочек поставок и даже обеспечив себе более здоровое и способное население. Эти технологические прорывы также приведут к тому, что биотехнологический сектор станет основным фактором общей конкурентоспособности экономики США.

Рекомендация: Уделять приоритетное внимание развитию передовой биотехнологической экосистемы НИОКР

Соединенные Штаты должны инвестировать в ключевые платформы, которые лучше позиционируют американскую академическую и коммерческую биотехнологическую индустрию, чтобы извлечь выгоду из достижений ИИ в биологии. Он должен специально стремиться поддерживать платформы, которые объединяют биоданные, и в частности генетические данные, безопасным образом, чтобы повысить способность американских исследователей использовать ИИ для содействия прорывным биотехнологическим исследованиям и инновациям. Кроме того, Соединенным Штатам следует поддерживать усилия по расширению масштабов и усложнению американской политики. возможности биофабрикации для обеспечения того, чтобы она могла идти в ногу с предстоящими научными достижениями. Она должна, в частности, поддерживать усилия по преобразованию биотехнологической отрасли от ее нынешних вертикально интегрированных моделей и поощрять развитие многочисленных стандартизированных коммерческих биофабрик. Это расширило бы доступ к передовым инструментам биофабрикации среди стартапов и лабораторий, позволив фирмам быстро проектировать новые молекулы и материалы через облако и размещать немедленные заказы на изготовление.

Действия для Конгресса и Министерства здравоохранения и социальных служб:

• Финансировать и создать биобанк мирового уровня для генетических данных.

Конгресс должен финансировать усилия по созданию биобанка мирового уровня в рамках Национальных институтов здравоохранения (NIH). Нынешняя ведущая генетическая база данных США, GenBank, недофинансирована, труднодоступна и плохо курируется, особенно по сравнению с другими ведущими генетическими базами данных, такими как Британский БиоБанк или Китайский Национальный генбанк. Объект должен быть надежно и легко доступен законным исследователям; содержать широкий спектр целых геномов человека, животных и растений, включая деидентифицированные метаданные о фенотипах; и агрегировать другие открытые и потенциально даже проприетарные наборы данных для специализированного использования. Он также должен включать в себя надежную защиту конфиденциальности генетических данных человека. Создание и укомплектование персоналом такого предприятия, вероятно, потребует бюджета примерно в 100 миллионов долларов в год, помимо первоначальных затрат на строительство.

• Прямое финансирование для поддержки передовых биотехнологических производственных инициатив через такие организации, как BARDA.

Министерство здравоохранения и социальных служб должно направлять средства на поддержку передовых инициатив в области биотехнологического производства через такие структуры, как Управление перспективных биомедицинских исследований и разработок (BARDA), а Конгресс должен уделять приоритетное внимание таким инициативам в будущих законопроектах о расходах, связанных со здравоохранением. Это может принять форму финансовых стимулов для передовых биотехнологических фирм, ориентированных на сложные, гибкие, облачные технологии производства, или финансирования НИОКР для поддержки передовых производственных технологий.

Рекомендация: Приоритетность передовых биотехнологических возможностей как Императива национальной безопасности и экономической конкурентоспособности

Растущее значение биотехнологического лидерства для здравоохранения, продовольствия, производства и науки также делает императивом национальной безопасности, чтобы Соединенные Штаты предприняли активные шаги для содействия долгосрочному лидерству США в этой области. Достижения в области биотехнологии также создадут новые вызовы национальной безопасности, начиная от искусственных патогенов и заканчивая усилением физиологических или умственных способностей человека. Соединенные Штаты в настоящее время не готовы решать такие проблемы, и биологические угрозы редко были приоритетной проблемой для сообщества национальной безопасности США. Пандемия COVID-19 ясно показывает, что Соединенные Штаты должны думать об угрозах национальной безопасности более широко, чем это было в прошлом, и что биологические угрозы, в частности, могут привести к значительным издержкам для американского общества и безопасности.

Американские конкуренты видят потенциал ИИ для стимулирования новых, трансформационных достижений в биотехнологии. Китай, в частности, активно стремится к глобальному лидерству в обеих областях, рассматривает свои стратегии ИИ и биотехнологии как взаимоукрепляющие и считает, что синергия между ними приведет к военному преимуществу. Китай также сталкивается с меньшим количеством барьеров для сбора, использования и объединения биологических данных человека, учитывая его пренебрежение личной неприкосновенностью и биоэтическими принципами. Глобальный охват китайского геномного гиганта BGI создает такие же угрозы в секторе биотехнологий, как и Huawei в секторе коммуникаций.

Действия для Администрации Президента:

• Обновить Национальную стратегию биологической защиты США, включив в нее дополнительные биологические угрозы с использованием искусственного интеллекта.

Совет национальной безопасности должен обновить свою Национальную стратегию биологической защиты, которая в настоящее время фокусируется

только на природных или искусственных патогенах, чтобы включить более широкое видение биологических угроз. Стратегия должна конкретно изучить, как ИИ может обеспечить новые биологические достижения, которые создают уникальные угрозы национальной безопасности, такие как улучшение человеческого потенциала, и как американские конкуренты могут использовать преимущества в биотехнологии или биоданных в качестве инструмента национальной власти. Он также должен конкретно рассмотреть вопрос о том, как ИИ может идентифицировать и противодействовать созданию передовых, сконструированных патогенов, которые нацелены на определенные элементы населения США или продовольственного снабжения. ИИ способствует быстрому развитию биотехнологической отрасли, и стратегия биологической защиты США должна развиваться вместе с ней.

• Поручить департаментам и агентствам определить приоритетность инициатив, способствующих лидерству США в области биотехнологий.

Руководство департаментами и агентствами для определения приоритетов инициатив, способствующих лидерству США в области биотехнологии, будет включать агрессивное стимулирование финансирования фундаментальных исследований в области биологии, в частности приложений биологии, использующих ИИ; сосредоточение ресурсов на прогнозировании того, как ИИ обеспечит будущие биотехнологические прорывы; и продолжение культивирования талантов как внутри, так и за пределами правительства, а также коммерческой деятельности на стыке ИИ и биологии. Для этого потребуется организация, наделенная полномочиями по координации деятельности в экономической, технологической сферах и сфере безопасности, например Совет по конкурентоспособности технологий, рекомендованный Комиссией.

Рекомендация

Рекомендация: Публично осветить связи BGI с китайским правительством

BGI является де-факто национальным чемпионом Китая в области генетического секвенирования и исследований и входит в число мировых лидеров в области секвенирования ДНК. Он имеет исследовательские связи с несколькими университетами США, включая Университет Вашингтона и Университет штата Вашингтон.14 BGI также воспользовалась существенной поддержкой китайского правительства, а также приобретением в 2013 году конкурирующей американской компании. твердая, Полная Геномика.15 Есть признаки того, что связи BGI с китайским правительством могут быть глубже, чем он публично заявляет, поскольку он построил и управляет China National GeneBank, национальной генетической базой данных китайского правительства, и использовал суперкомпьютеры, принадлежащие PLA, для обработки генетической информации.16 китайских дипломатов протолкнули созданные BGI тестовые наборы COVID-19, в том числе в США, и к августу 2020 года BGI «продала 35 миллионов быстрых тестовых наборов COVID-19 в 180 стран и построила 58 лабораторий в 18 странах.»17

BGI может служить, вольно или невольно, глобальным механизмом сбора генетических баз данных китайского правительства, предоставляя Китаю большее количество и разнообразие образцов генома человека, а также доступ к конфиденциальной личной информации о ключевых лицах по всему миру. Высшие уровни правительства Соединенных Штатов должны публично заявить об этих проблемах, чтобы повысить осведоМЛенность среди американских коммерческих и академических биотехнологических сообществ, а также союзников США, многие из которых в настоящее время имеют партнерские или деловые отношения с BGI.

Действия для Государственного департамента:

• Запустите стратегическую коммуникационную кампанию, чтобы публично подчеркнуть связи между китайским правительством и BIG.

Госсекретарь должен лично выразить озабоченность по поводу связей BGI с китайским правительством и поручить Департаменту провести стратегическую коммуникационную кампанию, чтобы подчеркнуть эти связи и

предупредить об опасности получения китайским правительством личной генетической информации через BGI. Департамент также должен предупредить BGI и китайское правительство, что он будет внимательно следить за деятельностью BGI, и что если BGI будет использоваться в качестве аппарата массового сбора ДНК для китайского правительства, он может столкнуться с дополнительными регулирующими действиями США.

Рекомендация: Продолжать глобальное сотрудничество в области Интеллектуального мониторинга заболеваний

Переходя к более конкурентоспособному национальному подходу к политике в области биотехнологии, Соединенные Штаты должны также продолжать усилия по укреплению глобального сотрудничества в области мониторинга заболеваний. Объединив существующие данные о здоровье с открытым исходным кодом с улучшенными сигналами раннего предупреждения и данными о зоонозных побочных эффектах и передаче новых вирусов, правительства смогут лучше использовать ИИ для прогнозирования и сдерживания будущих пандемий. Сочетание повышения прозрачности и обмена данными о вспышках заболеваний с инструментами искусственного интеллекта, которые могут улучшить раннее выявление вспышек и способствовать мониторингу заболеваний в режиме реального времени, может принести существенную пользу глобальному общественному здравоохранению, если все страны, включая Китай, будут добросовестно участвовать в этом процессе.

Меры для государственных департаментов здравоохранения и социальных служб:

- Поддерживать многосторонние усилия по содействию интеллектуальному мониторингу заболеваний.

Государственные департаменты, департаменты здравоохранения и социальных служб должны возглавлять и поддерживать многосторонние усилия по содействию интеллектуальному мониторингу заболеваний. В частности, Соединенным Штатам следует продолжать усилия по интеграции и

стандартизации международных наборов данных, связанных со здоровьем, и объединению их с глобальными данными о зоонозных побочных эффектах, чтобы позволить использовать технологии искусственного интеллекта для создания общих, прогнозирующих, глобальных инструментов мониторинга заболеваний.

Обеспечение лидерства США в области квантовых вычислений

Квантовые вычисления обладают потенциалом для создания новых угроз и возможностей национальной безопасности путем повышения скорости и точности существующих систем искусственного интеллекта и создания новых возможностей, которые могут коренным образом изменить стратегическую среду. Например, квантовые компьютеры могут быть в состоянии более эффективно оптимизировать логистику для военных или открыть новые материалы для систем вооружения. Квантовые датчики и средства связи также готовы революционизировать сбор и передачу конфиденциальной информации, что напрямую влияет на то, как ИИ обучается и развертывается в случаях использования национальной безопасности. Неспособность увеличить инвестиции в НИОКР материалов и компонентов для квантовых компьютеров, программных средств с открытым исходным кодом, а гибридные квантово-классические алгоритмы, использующие шумные квантовые компьютеры промежуточного масштаба, могут сделать Соединенные Штаты уязвимыми для стратегической неожиданности со стороны конкурентов.

Рекомендация: Переход от фундаментальных исследований к применению квантовых вычислений в области национальной безопасности

Несмотря на то, что Соединенные Штаты имеют хорошие возможности воспользоваться своими ранними успехами в фундаментальной науке квантовых вычислений, американское правительство должно сосредоточить свое внимание на разработке приложений для обеспечения национальной безопасности или рискнуть отстать от стратегических конкурентов. В частности, Китай сделал значительные инвестиции в военное применение квантовых вычислений в попытке компенсировать сильные стороны США.

Министерство обороны (МО) все еще совершенствует свой подход к быстрому переходу коммерческих технологий от исследований к полевым работам в дорогостоящих, аппаратно-интенсивных секторах, таких как квантовые вычисления. В долгосрочной перспективе Министерство обороны должно уделять приоритетное внимание усилиям по быстрому приобретению технологий в своих инновационных офисах, но этот процесс может занять несколько лет целенаправленных усилий. Тем временем объявления о приоритетных заявках помогут стимулировать инвестиции частного сектора и инновации в области квантовых вычислений, несмотря на отсутствие интегрированного механизма закупок технологий.

Действия для президента:

• Президент должен поручить департаментам и ведомствам объявить приоритетные варианты использования квантовых компьютеров.

Национальное квантовое координационное бюро (NQCO) должно координировать усилия департаментов и учреждений, представленных в Подкомитете Национального научно-технического совета (NSTC) по квантовой информатике (QIS), по объявлению своих приоритетных вариантов использования квантовых компьютеров. Отражая совокупные взгляды федеральных структур, взаимодействующих с частным сектором, это будет сигнализировать о том, что существует рынок для практического применения квантовых вычислений, ставить четкие и конкретные цели для частного сектора и стимулировать дополнительные частные инвестиции. Некоторые приложения квантовых компьютеров могут быть слишком чувствительными, чтобы раскрывать их публично, но те, которые могут быть объявлены, дадут направление частному сектору и облегчат коммерциализацию квантовых компьютеров, которые затем могут быть применены к случаям использования национальной безопасности.

Рекомендация: Способствовать созданию Динамичной Отечественной экосистемы Квантового производства

Из-за стратегических последствий квантовых вычислений и их применения к ИИ Соединенные Штаты должны предпринять шаги сейчас, чтобы закрепить свой долгосрочный статус мирового лидера в области проектирования и производства квантовых процессоров (QPU). Чтобы избежать ситуации, в которой в настоящее время находится полупроводниковая промышленность США, Соединенные Штаты должны создать надежные и надежные источники критических материалов и компонентов QPU, начиная от производственного оборудования и заканчивая сверхпроводниками и холодильниками для разбавления. Хотя эти материалы и компоненты, возможно, еще не представляют собой дроссельные точки, они неизбежно станут более специализированными по мере дальнейшего развития производственных процессов, необходимых для проектирования и производства QPU. Вместо того чтобы перестраивать всю цепочку поставок для QPU, Соединенные Штаты должны работать со своими союзниками над созданием устойчивой сети поставщиков критически важных компонентов, которые непосредственно влияют на национальную безопасность США.

Однако надежной цепочки поставок недостаточно для обеспечения лидерства США в области квантовых вычислений. Чтобы извлечь выгоду из будущих прорывов в этой области, Соединенные Штаты должны создать надежную внутреннюю экосистему для исследований, разработок и применения квантовых компьютеров, привлекающую талантливых специалистов высшего уровня со всего мира. Правительство США должно предложить стимулы для исследований и разработок квантовых компьютеров и их компонентов, одновременно создавая спрос на применение квантовых технологий для обеспечения национальной безопасности. Консорциум квантового экономического развития (QED-C), предложенный в Законе о Национальной квантовой инициативе (NQI) 2018 года, является важным шагом на пути к расширению лидерства США в области компьютерного оборудования следующего поколения на долгие годы.

Действия для Конгресса:

• Принять пакет положений, стимулирующих отечественное проектирование и производство квантовых компьютеров и составляющих их материалов.

Налоговый кредит на расходы, произведенные в Соединенных Штатах на исследования и разработки, производство оборудования и обучение рабочей силы, связанные с разработкой квантовых компьютеров, является необходимым, хотя и недостаточным шагом для поддержания конкурентоспособности США в этой области. Это положение может быть смоделировано на основе Альтернативного упрощенного кредита (ASC), который предоставляет кредит в размере 14% расходов на НИОКР сверх 50% расходов базового периода. Чтобы помочь стартапам, находящимся на переднем крае исследований и разработок, получить финансирование, позволяющее им масштабироваться, США Правительство также должно предоставлять кредитные гарантии и долевое финансирование.

Рекомендация: Сделать квантовые вычисления доступными для исследователей через Национальный исследовательский ресурс искусственного интеллекта (NAIRR)

Несмотря на последние достижения в области квантового оборудования и программного обеспечения, отказоустойчивые квантовые компьютеры (FTQCs), способные выполнять задачи общего назначения, вряд ли заменят классические компьютеры в ближайшее время. В ближайшей перспективе Соединенные Штаты должны инвестировать в шумные квантовые компьютеры промежуточного масштаба (NISQ), способные выводить вероятностные решения из несовершенных кубитов. Гибридные квантово-классические методы также показали себя многообещающими, когда классические компьютеры делегируют определенные задачи специально построенным квантовым устройствам в рамках одного и того же рабочего процесса. Однако ресурсы, пригодные для разработки такого типа программного обеспечения, не являются легкодоступными. Сделав классические и квантовые компьютеры

доступными в одном рабочем процессе, правительство США снизило бы барьеры для инноваций для стартапов в области квантовых вычислений и привлекло бы таланты высшего уровня со всего мира. Возникшее в результате этого государственно-частное партнерство также будет способствовать коммерциализации квантовых компьютеров и поможет правительству США использовать эти продукты для целей национальной безопасности.

Действия для Исполнительной власти:

• Сделать классические и квантовые компьютеры доступными в одном рабочем процессе через Национальный исследовательский ресурс ИИ.

Предоставляя доступ как к классическим, так и к квантовым компьютерам через Национальный исследовательский ресурс ИИ (NAIRR), который Комиссия рекомендовала создать в своих Рекомендациях за первый квартал и более подробно описывает в главе 11 настоящего доклада, правительство США поможет исследователям из промышленности, академических кругов и правительства создавать и тестировать программные средства и алгоритмы, которые используют как классические, так и квантовые компьютеры гибридным образом. Эти типы приложений, вероятно, будут ближайшим вариантом использования квантовых компьютеров.

Обеспечение лидерства США в области телекоммуникаций 5G

Системы искусственного интеллекта требуют высокоточного зондирования, а также быстрых, безопасных и защищенных сетей. Это императив национальной безопасности для американских военных и нации в целом, чтобы иметь доступ к мощной сети 5G, чтобы обеспечить будущие возможности искусственного интеллекта и обеспечить доверие к сети. Соединенные Штаты должны сохранить этот доступ и доверие, создавая коммерческие сети 5G внутри страны и на международном уровне.

Использования Спектра

Медленное развертывание сетей 5G в США по сравнению с Китаем рискует подорвать достижения США в области искусственного интеллекта, как

в государственном, так и в частном секторе.30 Спектр суб-6 ГГц, иногда называемый средней полосой или полосой спектра «златовласки», является критической частью спектра как для МО, так и для коммерческих операций 5G. Спектр суб-6 ГГц имеет решающее значение для гражданской связи 5G, поскольку он сочетает в себе высокую скорость передачи данных с хорошей дальностью и проникновением. В рамках МО он также уже используется многими радиолокационными и коммуникационными системами, поскольку он также сочетает в себе высокую способность различения с дальними операциями. Отчасти из-за своей важности для военных операций Министерство обороны сохранило исключительный доступ к значительным частям среднечастотного спектра, что ограничивает коммерческое использование. К сожалению, отсутствие коммерческой доступности среднечастотного спектра в США существенно замедляет развертывание сетей 5G внутри страны. Учитывая, что суб-6 ГГц имеет важное значение для зондирования с использованием радаров и гражданской связи, совместное использование спектра между Министерством обороны и частным сектором является идеальным подходом к обеспечению доступа для обеих целей таким образом, чтобы сбалансировать национальную безопасность и экономические интересы.

Несколько правительственных учреждений США работают над решением этой проблемы, развивая возможности совместного использования спектра в диапазоне от 3 до 6 ГГц. В 2015 году Федеральная комиссия по связи (FCC) учредила Гражданскую широкополосную радиосвязь (CBRS), первую американскую модель совместного использования спектра.33 С тех пор Национальное управление телекоммуникаций и информации (NTIA) изучало и сотрудничало с Министерством обороны и FCC по максимизации возможностей совместного использования спектра. CBRS обеспечивает совместное федеральное и нефедеральное использование полосы частот. Эта работа позволяет США Военно-морской флот и негосударственные провайдеры разделят полосу 3550-3700 МГц на три динамически управляемых уровня:

военно-морской флот будет поддерживать приоритетный доступ в первую очередь, за ним следуют компании и организации, которые покупают лицензии на приоритетный доступ, и, наконец, компании и организации, которые регистрируются бесплатно. FCC провела свой первый аукцион на получение лицензий приоритетного доступа для этой полосы в июле 2020 года, который собрал более 4,5 миллиардов долларов за счет продажи 20 625 лицензий. Это многообещающее, но скромное начало, и эти усилия должны быть расширены до большей части спектра средней полосы, чтобы быть конкурентоспособными с Китаем. Для достижения совместного использования спектра на конкурентном уровне потребуется технический анализ и взаимодействие с промышленностью. Комплексный процесс будет иметь решающее значение для обеспечения того, чтобы МО поддерживало доступ к спектру, необходимому для обеспечения операционной эффективности, а также расширяло коммерческий доступ к спектру для гражданских сетей 5G.36

Действия для NTIA, FCC и Министерства обороны:

• Расширение программ совместного использования спектра под руководством NTIA, FCC и Министерства обороны, начиная с однолетней демонстрационной программы совместного использования спектра 5G.

Комиссия настоятельно призывает NTIA, FCC и Министерство обороны совместно расширить программы совместного использования спектра, такие как CBRS, и работать над лицензированием дополнительного спектра суб-6 ГГц для операторов беспроводной связи и производителей оборудования для коммерческого использования 5G. Совместное использование и лицензирование дополнительного среднечастотного спектра обеспечит неограниченный доступ Минобороны в случае чрезвычайной ситуации, а также откроет 5G для коммерческого использования. Однако существующие возможности совместного использования спектра должны быть дополнительно проанализированы, протестированы и продемонстрированы, прежде чем их можно будет масштабировать. Комиссия поддерживает годичную демонстрационную программу, включающую NTIA, FCC, DoD и

промышленность для оценки возможностей сети и ее способности динамично обмениваться спектром между государственными и гражданскими пользователями. В случае успеха такая сеть будет быстро масштабироваться с помощью коммерчески доступного оборудования.

Продвигать лидерство США в других Ключевых развивающихся технологиях

Искусственный интеллект, микроэлектроника, биотехнологии, квантовые вычисления и телекоммуникации 5G-не единственные новые технологии, которые будут поддерживать национальную конкурентоспособность США в 21 веке. Комиссия оценивает, что полный спектр новых технологий, ключевых для технологического лидерства США, расширяется и включает автономию и робототехнику, передовые производственные и энергетические системы. Поэтому Комиссия рекомендует ряд мер для обеспечения лидерства США в этих дополнительных ключевых новых технологиях.

Рекомендация: Стимулировать разработку программных платформ мирового класса для робототехники и автономных систем.

Автономные системы, которые полагаются на робототехнику для выполнения задач в реальном мире, применяются ко всему от передового производства до боевых действий.38 Поскольку ИИ продолжает совершенствовать способность этих систем соответствовать человеческим возможностям или превосходить их, Соединенные Штаты должны позиционировать себя в качестве ведущего производителя и разработчика роботизированного оборудования и программного обеспечения для гражданских и военных целей. Соединенные Штаты в настоящее время отстают от таких стран, как Япония и Корея, по производству и установке промышленных роботов, а Китай объявил робототехнику основной отраслью. По мере того как Соединенные Штаты перестраивают некоторые стратегические цепочки поставок и усиливают свою зависимость от автономных систем, постоянный доступ к новейшей робототехнике станет императивом национальной безопасности.

Деятельность Национального института стандартов и технологий:

• Стимулирование разработки американскими фирмами программных платформ мирового уровня для робототехнических систем.

Разрабатывая программные платформы, на которых строятся основные робототехнические возможности, американские фирмы будут иметь хорошие возможности для формирования следующей волны индустриализации. Правительство США должно расширить сотрудничество с промышленностью в области фундаментальных исследований и разработок, установить международные стандарты и обмениваться данными, относящимися к разработке робототехнических систем, расширяя работу Отдела интеллектуальных систем Национального института стандартов и технологий (NIST). США правительство также должно стимулировать скорейшее внедрение робототехнических систем в государственном и частном секторах путем создания рынков в областях, готовых к автоматизации. Эти усилия дадут ценные данные и опыт в области масштабирования автоматизации и облегчат применение робототехники в смежных секторах. Многосторонний подход в этом направлении позволит американской промышленности более эффективно конкурировать на рынке программного обеспечения для робототехнических систем-стратегически важной области, совместимой с существующими сильными сторонами США.

Передовое Производство

Рекомендация: Ускорить Аддитивное производство Производство устаревших деталей По всему Министерству обороны

Способность производить высокотехнологичную продукцию внутри страны имеет решающее значение для безопасности страны и ее экономической производительности. Соединенные Штаты должны стремиться развивать производственный потенциал в отраслях, которые необходимы для реагирования на кризис или которые слишком долго не будут задействованы в случае затяжного конфликта. Инновации также выигрывают от совместного размещения фирм, занимающихся технологическим проектированием, и фирм, производящих готовую продукцию, что обеспечивает быструю обратную связь и непрерывную итерацию при проектировании продукта. Эта связь особенно важна в оборонной сфере, где осуществляется связь между исследователями, конструкторами, а производители могут помочь быстро перевести технологию из лаборатории в поле. Однако Соединенные Штаты отказались от лидерства в производстве высокотехнологичных отраслей, в которых работают высококвалифицированные рабочие, в пользу таких высокооплачиваемых стран, как Германия и Япония. Тем временем Китай и другие страны с более низкой заработной платой продвигаются вверх по цепочке создания стоимости от низкозатратных производственных процессов, таких как сборка, к более сложным технологиям. Хотя сбои в цепочке поставок, вызванные пандемией COVID-19, могут привести к возвращению некоторых производственных предприятий в Соединенные Штаты., более широкая тенденция к офшорингу производства технологий нового поколения, по-видимому, сохранится, если правительство США не примет соответствующих мер.

Действия для Министерства обороны:

• Ускорить аддитивное производство устаревших деталей по всему Министерству обороны.

Аддитивное производство и 3D-печать обладают потенциалом для трансформации обрабатывающей промышленности, позволяя быстро

производить сложные объекты по требованию и в момент необходимости. Хотя существующие 3D-принтеры не могут сравниться по качеству с передовыми традиционными технологиями, ИИ продемонстрировал потенциал значительного повышения точности 3D-печати. Министерство обороны должно активно поддерживать совершенствование 3D-печати путем выявления всех устаревших деталей в активных системах вооружения, пригодных для производства аддитивным производством и 3D-принтерами, и взять на себя обязательство сделать это к 2025 году.

Энергетические системы

Рекомендация: Разработка и внутреннее производство Технологий хранения энергии для удовлетворения рыночного спроса США к 2030 году

Дешевый и надежный доступ к энергии имеет решающее значение для национальной безопасности США. Хотя Соединенные Штаты находятся на переднем крае разведки, добычи и переработки нефти и газа и обладают значительными внутренними запасами, Китай, безусловно, является ведущим производителем возобновляемых источников энергии и инвестирует значительные средства в передовые технологии хранения энергии, такие как батареи и составляющие их материалы.50 Поскольку стоимость прерывистых возобновляемых источников продолжает падать, Соединенные Штаты должны взять на себя обязательства по разработке и развертыванию следующего поколения устройств хранения энергии-от долговременных стационарных применений до аккумуляторных батарей для электромобилей.

Действия для Конгресса:

• Финансировать инициативу Министерства энергетики по разработке и отечественному производству технологий хранения энергии для удовлетворения спроса американского рынка к 2030 году.

Повышение стоимости и плотности энергии технологий хранения будет способствовать прогрессу в различных секторах-от электромобилей до распределенной генерации энергии. Министерство энергетики (DoE) поставило перед собой амбициозную цель разработки и внутреннего производства

технологий хранения, способных удовлетворить весь рыночный спрос США к 2030 году. Конгресс должен полностью финансировать федеральные НИОКР, необходимые для достижения дорожной карты DoE Energy Storage Grand Challenge к 2030 году, и установить соответствующие стимулы для коммерциализации полученных технологий.

Дальнейшее рассмотрение дополнительных технологий и заключение

Хотя Комиссия считает, что восемь новых технологий, рассмотренных выше и в других разделах настоящего доклада,—искусственный интеллект, микроэлектроника, биотехнологии, квантовые вычисления, телекоммуникации 5G, автономия и робототехника, передовое производство и энергетические системы—будут иметь решающее значение для будущей национальной конкурентоспособности, этот список ни в коем случае не является исчерпывающим. Другие новые технологии и платформы—от цифровых валют и других видов финансовых технологий до космических систем—вероятно, также будут играть важную роль в продвижении экономики США и ее национальной безопасности. И, несомненно, существуют технологии, которые еще предстоит создать и которые в ближайшем будущем окажут преобразующее воздействие на жизнь и безопасность американских граждан.

Мы находимся в начале новой эры, в которой технологии не только являются основным двигателем глобальных рынков и геополитики, но и развиваются и появляются быстрее, чем когда-либо прежде. По мере ускорения темпов технологического развития и увеличения числа технологий двойного назначения угрозы техно-национальной безопасности будут продолжать множиться. Чтобы справиться с этой задачей, правительство США должно постоянно оценивать новые технологические достижения, чтобы определить их потенциал для разрушения промышленности, изменения экономики и преобразования национальной безопасности.

Процесс сканирования технологического горизонта, прогнозирования и проактивной разработки политики для решения предстоящих угроз национальной безопасности, связанных с новыми технологиями, должен стать

неотъеМЛемым компонентом процесса национальной безопасности США. Это не только необходимо, но и крайне необходимо. Если правительство США будет ждать, чтобы приспособиться к этой новой реальности, пока последующая комиссия не вынесет аналогичную рекомендацию, оно, скорее всего, будет играть в технологическое догоняние с позиции слабости национальной безопасности. По мере развития существующих и появления новых технологий связь между технологиями и национальной безопасностью будет только укрепляться, а потребность Соединенных Штатов в сохранении общего технического лидерства будет только возрастать.

Ссылки и ресурсы:

1. Комиссия определила их как необходимые для общего технологического лидерства США в своем Промежуточном докладе за 2019 год. См. Промежуточный отчет NSCAI от 31 ноября 2019 года, https://www.nscai.gov/previous-reports/.

2. Краткое изложение Стратегии национальной обороны Соединенных Штатов Америки на 2018 год, Министерство обороны США на 3 (2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

3. 2019 финансовый год Промышленные возможности: Доклад Конгрессу, Министерство обороны США в 132 (23 июня 2020 года), https://www.businessdefense.gov/Portals/51/Documents/Resources/USA000954-20%20RPT%20Subj%20FY19%20ICR%2007092020.pdf?ver=2020-07-10-124452-180.

4. 83 Fed. Reg. 58201, Review of Controls for Certain Technologies, U. S. Department of Commerce: Bureau of Industry and Security (Nov. 19, 2018), https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies.

5. Рекомендации по укреплению американского лидерства в отраслях будущего, Президентский совет советников по науке и технике (июнь 2020 г.),

https://science.osti.gov/-
/media/_/pdf/about/pcast/202006/PCAST_June_2020_Report.pdf.

6. S. 3832, 116-й конг. (2020), https://www.congress.gov/bill/116th-congress/senate-bill/3832.

7. Национальная стратегия в области критических и новых технологий, Белый дом на A-1 (октябрь 2020 г.), https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/10/National-Strategy-for-CET.pdf.

8. Дональд Дж. Трамп, Исполнительный указ 13922: Делегирование полномочий В соответствии с Законом об оборонном производстве Главному исполнительному директору Международной финансовой корпорации развития Соединенных Штатов Для реагирования на вспышку COVID-19, Белый дом (14 мая 2020 года), https://www.federalregister.gov/documents/2020/05/19/2020-10953/delegating-authority-under-the-defense-production-act-to-the-chief-executive-officer-of-the-united.

9. Для сравнения, китайское правительство выделило приблизительно 117 миллионов долларов первоначального финансирования Китайскому Национальному генбанку для его строительства и создания. См. Чжуан Пинхуэй, Китай Открывает Первый Национальный банк генов, нацеленный на размещение сотен миллионов образцов, South China Morning Post (22 сентября 2016 г.) https://www.scmp.com/news/china/article/2021623/chinas-noahs-ark-first-national-gene-bank-opens-shenzhen.

10. Эльза Кания, Minds at War: China ' s Pursuit of Military Advantage Through Cognitive Science and Biotechnology, Prism (Jan. 2020), https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3_Kania_82-101.pdf.

11. Эта рекомендация включена в главу 1 настоящего доклада.

12. Национальная Стратегия Биологической защиты, Белый дом (2018), https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Biodefense-Strategy.pdf.

13. Дополнительную информацию о предлагаемом Совете по конкурентоспособности технологий см. в главе 9 настоящего доклада.

14. См., например, BGI & US Collaborate on Precision Medicine Development, UW Medicine (10 мая 2016 г.), https://newsroom.uw.edu/story/bgi-uw-collaborate-precision-medicine-development.

15. В 2010 году BGI получила кредит в размере 1,5 миллиарда долларов от государственного банка развития Китая. Точные размеры государственных субсидий КРУПНЫМ компаниям неизвестны, но, скорее всего, существенны. См. Кирсти Нидхэм, Специальный репортаж: COVID Открывает новые двери для китайского Генного гиганта, Reuters (5 августа 2020 года), https://www.reuters.com/article/us-health-%20coronavirus-bgi-specialreport/special-report-covid-opens-new-doors-for-chinas-gene-giant-idUSKCN2511CE; см. Также Antonio Regaldo, China BGI Says It Can Sequence a Genome for Just $100, MIT Technology Review (Feb. 26, 2020), https://www.technologyreview.com/2020/02/26/905658/china-bgi-100-dollar-genome/.

16. Китайский Национальный Генный банк Официально открывается, BGI (22 сентября 2016 года), https://www.bgi.com/us/company/careers/china-national-genebank-officially-opens/.

17. См. Кирсти Нидхэм, Специальный репортаж: COVID Открывает новые двери для китайского Генного гиганта, Reuters (5 августа 2020 года), https://www.reuters.com/article/us-health-coronavirus-bgi-specialreport/special-report-covid-opens-new-doors-for-chinas-gene-giant-idUSKCN2511CE; см. Также Jeanne Whalen & Elizabeth Dwoskin, Калифорния Отклонила предложение китайской компании помочь с тестированием на коронавирус. Был ли Это Правильный Шаг? Washington Post (2 июля 2020 года), https://www.washingtonpost.com/business/2020/07/02/china-bgi-california-testing/.

18. Дополнительную информацию о сотрудничестве по вопросам, связанным с ИИ и глобальным здравоохранением, см. в главах 9 и 15 настоящего доклада.

19. Pontus Vikstål, et al., Applying the Quantum Approximate Optimization Algorithm to the Tail-Assignment Problem, Physical Review Applied Vol. 14, Iss. 3 (Sept. 3, 2020), https://doi.org/10.1103/PhysRevApplied.14.034009; HeMa, et al., Quantum Simulations of Materials on Near-Term Quantum Computers, npj Computational Materials (2 июля 2020 г.), https://doi.org/10.1038/s41524-020-00353-z.

20. C. L. Degen, et al., Quantum Sensing, arXiv (7 июня 2017 г.), https://arxiv.org/pdf/1611.02427.pdf; Juan Yin, et al., Entanglement-Based Secure Quantum Cryptography over 1120 Kilometers, Nature 582, 501-505 (15 июня 2020 г.), https://doi.org/10.1038/s41586-020-2401-y.

21. В декабре 2020 года группа исследователей из Китая продемонстрировала квантовое преимущество на фотонном квантовом компьютере. См. HanSen Zhong, et al., Quantum Computational Advantage Using Photons, Science (Dec. 18, 2020), https://science.sciencemag.org/content/370/6523/1460.

22. Эльза Б. Кания и Джон Костелло, Квантовая гегемония? Амбиции Китая и вызов инновационному лидерству США, CNAS (12 сентября 2018 г.), https://www.cnas.org/publications/reports/quantum-hegemony.

23. Дополнительную информацию и взгляды NSCAI на квантовые вычисления, искусственный интеллект и национальную безопасность см. в Промежуточном отчете и Рекомендациях третьего квартала NSCAI at 154-163 (октябрь 2020 г.), https://www.nscai.gov/previous-reports/.

24. Применение квантовых технологий: Резюме, Совет по оборонным наукам на С-1 (октябрь 2019 года), https://dsb.cto.mil/reports/2010s/DSB_QuantumTechnologies_Executive%20Summary_10.23.2019_SR.pdf.

25. Дарио Гил, Как обеспечить квантовое будущее США, Scientific American (20 августа 2020 года), https://www.scientificamerican.com/article/how-to-ensure-the-uss-quantum-future/.

26. Двухпартийный Закон о национальной квантовой инициативе 2018 года побудил к ряду шагов, которые устанавливают квантовые вычисления в качестве стратегического приоритета для Соединенных Штатов. Министерство энергетики (DoE) объявило о выделении 625 миллионов долларов на создание пяти исследовательских центров квантовой информатики в течение пяти лет под руководством национальных лабораторий. Национальный научный фонд (NSF) объявил о выделении 75 миллионов долларов на создание трех институтов Quantum Leap Challenge за тот же период. Наконец, президентский бюджет на 2021 финансовый год рекомендовал удвоить федеральные инвестиции в квантовые технологии к 2022 году. Эти постоянные инвестиции необходимы для определения полного потенциала квантовых вычислений и сохранения лидерских позиций Соединенных Штатов в области компьютерного оборудования следующего поколения. Более подробную информацию см. в Pub. L. 115-368, National Quantum Initiative Act, 115th Cong. (2018), https://www.congress.gov/bill/115th-congress/house-bill/6227; Министерство энергетики Объявляет о выделении 625 миллионов долларов на Новые квантовые центры, Министерство энергетики США (10 января 2020 года), https://www.energy.gov/articles/department-energy-announces-625-million-new-quantum-centers; NSF Создает 3 Новых института для решения Критических задач в области квантовой информатики, Национальный научный фонд (21 июля 2020 года), https://www.nsf.gov/news/special_reports/announcements/072120.jsp Рекомендации по укреплению американского лидерства в отраслях будущего, Президентский совет советников по науке и технике на 13 (июнь 2020 года), https://science.osti.gov/-/media/_/pdf/about/pcast/202006/PCAST_June_2020_Report.pdf?la=en&hash=019A4F17C79FDEE5005C51D3D6CAC81FB31E3ABC.

27. Джон Прескилл, Квантовые вычисления в эпоху НИКА и за ее пределами arXiv at 4, 14 (30 июля 2018 года), https://arxiv.org/pdf/1801.00862.pdf.

28. Министерство энергетики и ВВС предлагают доступ к коммерческим квантовым возможностям, но этот доступ не является широко распространенным и не ориентирован на разработку гибридного квантово-классического программного обеспечения. См. Adrian Cho, After Years of Avoidance, Department of Energy Joins Quest to Development Quantum Computers, Science (Jan. 10, 2018), https://www.sciencemag.org/news/2018/01/after-years-avoidance-department-energy-joins-quest-develop-quantum-computers; Научно-исследовательская лаборатория ВВС присоединится к IBM Q Network в качестве первого возглавляемого Министерством обороны IBM Q Hub, Wright-Patterson AFB (Aug. 2, 2019), https://www.wpafb.af.mil/News/Article-Display/Article/1924271/air-force-research-laboratory-to-join-ibm-q-network-as-first-dod-led-ibm-q-hub/.

29. См. Рекомендации за первый квартал, NSCAI, 12-13 (март 2020 г.), https://www.nscai.gov/previous-reports/. В 2021 финансовом году Конгресс сделал первый шаг к выполнению рекомендаций Комиссии за первый квартал, создав целевую группу для разработки дорожной карты для НАИРР. См. Pub. L. 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021). В главе 11 настоящего доклада Комиссия настоятельно призывает Конгресс санкционировать и выделить средства, необходимые для немедленного осуществления «дорожной карты» целевой группы.

30. Дэн Стрампф, США против Китая в 5G: Битва еще не близка, Wall Street Journal (9 ноября 2020 года), https://www.wsj.com/articles/u-s-vs-china-in-5g-the-battle-isnt-even-close-11604959200.

31. Дана Дизи, Заявление Министерства обороны о среднечастотном спектре, Министерство обороны США (10 августа 2020 года), https://www.defense.gov/Newsroom/Speeches/Speech/Article/2307288/department-of-defense-statement-on-mid-band-spectrum.

32. Milo Medin & Gilman Louie, The 5G Ecosystem: Risks & Opportunities for DoD, Defense Innovation Board (3 апреля 2019),

https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF.

33. Обзор диапазона 3,5 ГГц, Федеральная комиссия связи США (23 апреля 2020 г.), https://www.fcc.gov/wireless/bureau-divisions/mobility-division/35-ghz-band/35-ghz-band-overview.

34. Эдвард Дроцелла и др., Техническая возможность совместного использования Федерального спектра с будущими коммерческими операциями в диапазоне 3450-3550 МГц, NTIA (27 января 2020 г.), https://www.ntia.gov/report/2020/technical-feasibility-sharing-federal-spectrum-future-commercial-operations-3450-3550.

35. См. Публичное уведоМЛение: Аукцион Лицензий приоритетного доступа в диапазоне 3550-3650 МГц Закрывается, FCC (2 сентября 2020 г.), https://docs.fcc.gov/public/attachments/DA-20-1009A1.pdf.

36. В апреле 2019 года Совет по оборонным инновациям опубликовал доклад, в котором утверждалось, что статус-кво распределения спектра является неустойчивым, и Министерство обороны должно расширить свои операции по совместному использованию спектра ниже 6 ГГц, чтобы позволить Соединенным Штатам конкурировать с Китаем в области 5G. Milo Medin & Gilman Louie, The 5G Ecosystem: Risks & Opportunities for DoD, Defense Innovation Board (3 апреля 2019), https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF. Дополнительную информацию и мнения Комиссии по 5G см. в Рекомендациях за первый квартал, NSCAI at 54-57 (март 2020 г.), https://www.nscai.gov/previous-reports/.

37. Рекомендации по обеспечению лидерства США в области биотехнологий, квантовых вычислений и телекоммуникаций 5G можно найти выше. Рекомендации, касающиеся полупроводников и современного компьютерного оборудования, рассматриваются в главе 13 настоящего доклада.

38. Летнее исследование по автономии, Совет по науке обороны (июнь 2016 г.), https://dsb.cto.mil/reports/2010s/DSBSS15.pdf.

39. Китай владеет одной пятой мировых поставок промышленных роботов и стремится к тому, чтобы к концу 2020 года 45% его высокотехнологичных роботов производились внутри страны. См. Джонни Уильямсон, Как страны по всему миру инвестируют в исследования робототехники, The Manufacturer (10 июня 2020 года), https://www.themanufacturer.com/articles/how-nations-around-the-world-are-investing-in-robotics-research/.

40. Отдел интеллектуальных систем, NIST (последний доступ 2 февраля 2021 года), https://www.nist.gov/el/intelligent-systems-division-73500.

41. Например, Почтовая служба США может расширить свою пилотную программу автономных мобильных роботов с 25 сортировочных установок до всех сортировочных установок к 2025 году. Автономные мобильные роботы и почтовая служба, Управление Генерального инспектора почтовой службы США (9 апреля 2018 года), https://www.uspsoig.gov/sites/default/files/document-library-files/2019/RARC-WP-18-006.pdf.

42. Отчет по Исполнительному приказу 13806 определяет 10 архетипов производственного риска. См. Оценку и укрепление Производственной и оборонно-промышленной базы и Отказоустойчивости цепочек поставок Соединенных Штатов, Министерство обороны США (сентябрь 2018 г.), https://media.defense.gov/2018/oct/05/2002048904/-1/-1/1/assessing-and-strengthening-the-manufacturing-and%20defense-industrial-base-and-supply-chain-resiliency.pdf.

43. Стратегия американского лидерства в передовом производстве, Национальный совет по науке и технике (октябрь 2018 г.), https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/10/Advanced-Manufacturing-Strategic-Plan-2018.pdf; Gregory Tassey, Rationales and Mechanisms for Revitalizing US Manufacturing R&D Strategies, NIST (Jan. 29, 2010), https://www.nist.gov/system/files/documents/2017/05/09/manufacturing_strategy_paper_0.pdf.

44. Доклад Президенту об обеспечении американского лидерства в передовом производстве, Президентский совет советников по науке и технике (июнь 2011 г.), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/pcast-advanced-manufacturing-june2011.pdf; Advanced Manufacturing: A Snapshot of Priority Technology Areas Across the Federal Government, National Science and Technology Council (April 2016), https://www.manufacturing.gov/sites/default/files/2018-01/nstc_sam_technology_areas_snapshot.pdf.

45. Доклад Президенту об обеспечении американского лидерства в передовом производстве, Президентский совет советников по науке и технике на 3 июня 2011 года, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/pcast-advanced-manufacturing-june2011.pdf.

46. Передовое производство: Инновационные институты Продемонстрировали Первоначальные Достижения, но остаются проблемы в Измерении Производительности и обеспечении устойчивости, GAO-19-409 at 1 (23 мая 2019 года), https://www.gao.gov/assets/700/699310.pdf.

47. Аудит использования Минобороны аддитивного производства для вспомогательных частей, Генеральный инспектор Министерства обороны США (17 октября 2019 года), https://media.defense.gov/2019/Oct/21/2002197659/-1/-1/1/DODIG-2020-003.PDF.

48. Марк Андерсон, Задания 3D-Печати Более Точны С Помощью Машинного Обучения, IEEE Spectrum (19 Февраля 2020 Г.), https://spectrum.ieee.org/tech-talk/artificial-intelligence/machine-learning/3d-print-jobs-news-accurate-machine-learning.

49. Например, в августе 2020 года Министерство обороны напечатало первую металлическую деталь для реактивного двигателя B-52. См. Кайл Мизоками, Двигатель Старой школы, Который питает B-52, Получает обновление с 3D-печатью, Популярная механика (10 августа 2020 года),

https://www.popularmechanics.com/military/aviation/a33535790/air-force-3d-print-metal-part-turbofan-engine/.

50. Роберт Рапир, Десять Стран, Доминирующих В Производстве Ископаемого Топлива, Forbes (14 Июля 2019 Года), https://www.forbes.com/sites/rrapier/2019/07/14/ten-countries-that-dominate-fossil-fuel-production; Рейтинг стран, Международное агентство по возобновляемым источникам энергии, (последний доступ 2 февраля 2021 года), https://www.irena.org/Statistics/View-Data-by-Topic/Capacity-and-Generation/Country-Rankings.

51. Хранение энергии, Министерство энергетики США (последний доступ 2 февраля 2021 года), https://www.energy.gov/oe/energy-storage.

52. Грандиозная задача по хранению энергии: Дорожная карта, Министерство энергетики США (декабрь 2020 г.), https://www.energy.gov/sites/prod/files/2020/12/f81/Energy%20Storage%20Grand%20Challenge%20Roadmap.pdf.