Белый Дом **24 октября 2024**

Меморандум о развитии лидерства США в области искусственного интеллекта; использовании искусственного интеллекта для достижения целей национальной безопасности; и повышении безопасности, защищенности и надежности искусственного интеллекта

(машинный перевод, полый текст)

МЕМОРАНДУМ ДЛЯ ВИЦЕ-ПРЕЗИДЕНТА

ГОСУДАРСТВЕННЫЙ СЕКРЕТАРЬ

МИНИСТР КАЗНАЧЕЙСТВ

МИНИСТР ОБОРОНЫ

ГЕНЕРАЛЬНЫЙ ПРОКУРОРТ

МИНИСТР ТОРГОВЛИ

МИНИСТР ЭНЕРГЕТИКИ

МИНИСТР ЗДРАВООХРАНЕНИЯ И СОЦИАЛЬНЫХ СЛУЖБ

МИНИСТР ВНУТРЕННЕЙ БЕЗОПАСНОСТИ

ДИРЕКТОР УПРАВЛЕНИЯ ПО УПРАВЛЕНИЮ И БЮДЖЕТУ

ДИРЕКТОР НАЦИОНАЛЬНОЙ РАЗВЕДКИ

ПРЕДСТАВИТЕЛЬ США В ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ

ДИРЕКТОР ЦЕНТРАЛЬНОГО РАЗВЕДЫВАТЕЛЬНОГО УПРАВЛЕНИЯ

ПОМОЩНИК ПРЕЗИДЕНТА И РУКОВОДИТЕЛЬ АППАРАТНОЙ ГРУППЫ

ПОМОЩНИК ПРЕЗИДЕНТА ПО ВОПРОСАМ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

ПОМОЩНИК ПРЕЗИДЕНТА ПО ЭКОНОМИКЕ

ПОЛИТИКА И ДИРЕКТОР НАЦИОНАЛЬНОГО ЭКОНОМИЧЕСКОГО СОВЕТА

ПРЕДСЕДАТЕЛЬ СОВЕТА ЭКОНОМИЧЕСКИХ КОНСУЛЬТАНТОВ

ДИРЕКТОР УПРАВЛЕНИЯ ПОЛИТИКИ В ОБЛАСТИ НАУКИ И ТЕХНОЛОГИЙ

АДМИНИСТРАТОР АГЕНТСТВА США ПО МЕЖДУНАРОДНОМУ РАЗВИТИЮ

ДИРЕКТОР НАЦИОНАЛЬНОГО НАУЧНОГО ФОНДА

ДИРЕКТОР ФЕДЕРАЛЬНОГО БЮРО РАССЛЕДОВАНИЙ

НАЦИОНАЛЬНЫЙ КИБЕР-ДИРЕКТОР

ДИРЕКТОР УПРАВЛЕНИЯ ПОЛИТИКИ ГОТОВНОСТИ К ПАНДЕМИЯМ И РЕАГИРОВАНИЯ

ДИРЕКТОР АГЕНТСТВА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

ДИРЕКТОР НАЦИОНАЛЬНОГО АГЕНТСТВА ГЕОПРОСТРАНСТВЕННОЙ РАЗВЕДКИ

ДИРЕКТОР АГЕНТСТВА РАЗВЕДКИ МИНИСТЕРСТВА ОБОРОНЫ США

ТЕМА: Укрепление лидерства Соединенных Штатов в

Искусственный интеллект; использование искусственного интеллекта

Разведка для обеспечения национальной безопасности

Цели; и содействие безопасности, защищенности,

и надежность искусственного интеллекта

Раздел 1. Политика.

(a) Настоящий меморандум соответствует директиве, изложенной в подпункте 4.8 Указа 14110 от 30 октября 2023 года (Безопасная, надежная и заслуживающая доверия разработка и использование искусственного интеллекта). Настоящий меморандум содержит дальнейшие указания по надлежащему использованию моделей искусственного интеллекта (ИИ) и технологий с поддержкой ИИ в правительстве Соединенных Штатов, особенно в контексте систем национальной безопасности (СНБ), при одновременной защите прав человека, гражданских прав, гражданских свобод, конфиденциальности и безопасности в деятельности по обеспечению национальной безопасности с поддержкой ИИ. В секретном приложении к настоящему меморандуму рассматриваются дополнительные деликатные вопросы национальной безопасности, включая противодействие использованию ИИ противником, которое представляет риски для национальной безопасности Соединенных Штатов.

(b) Национальные институты безопасности США исторически побеждали в эпоху технологического перехода. Чтобы соответствовать меняющимся временам, они разрабатывали новые возможности, от подводных лодок и самолетов до космических систем и киберинструментов. Чтобы получить решающее преимущество и защитить национальную безопасность, они стали пионерами в области таких технологий, как радар, глобальная система позиционирования и ядерная тяга, и вывели эти с трудом завоеванные прорывы на поле боя. С каждой сменой парадигмы они также разрабатывали новые системы для отслеживания и противодействия попыткам противников использовать передовые технологии в своих интересах.

(c) ИИ стал технологией, определяющей эпоху, и продемонстрировал значительную и растущую значимость для национальной безопасности. Соединенные Штаты должны возглавить мир в ответственном применении ИИ для соответствующих функций национальной безопасности. ИИ, если его использовать надлежащим образом и по назначению, может принести большую пользу. При неправильном использовании ИИ может угрожать национальной безопасности Соединенных Штатов, укреплять авторитаризм во всем мире, подрывать демократические институты и процессы, способствовать нарушениям прав человека и ослаблять основанный на правилах международный порядок. Пагубные последствия могут иметь место даже без злого умысла, если системы и процессы ИИ не имеют достаточной защиты.

(d) Недавние инновации подстегнули не только рост использования ИИ в обществе, но и смену парадигмы в области ИИ — которая произошла в основном за пределами правительства. Эта эра разработки и развертывания ИИ опирается на беспрецедентные агрегации специализированной вычислительной мощности, а также на глубокие научные и инженерные знания, большая часть которых сосредоточена в частном секторе. Эта тенденция наиболее очевидна с появлением больших языковых моделей, но она распространяется на более широкий класс все более универсальных и вычислительно интенсивных систем. Правительство Соединенных Штатов должно срочно рассмотреть, как эта текущая парадигма ИИ конкретно может преобразовать миссию национальной безопасности.

(e) Предсказать технологические изменения с уверенностью невозможно, но основополагающие драйверы, которые лежали в основе недавнего прогресса ИИ, не показывают никаких признаков ослабления. Эти факторы включают в себя комплексные алгоритмические улучшения, все более эффективное вычислительное оборудование, растущую готовность промышленности существенно инвестировать в исследования и разработки и расширение наборов обучающих данных. ИИ в рамках текущей парадигмы может продолжать становиться все более мощным и универсальным. Разработка и эффективное использование этих систем требует развивающегося массива ресурсов, инфраструктуры, компетенций и рабочих процессов, которые во многих случаях отличаются от того, что требовалось для использования предыдущих технологий, включая предыдущие парадигмы ИИ.

(f) Если правительство Соединенных Штатов не будет действовать ответственно и быстро в партнерстве с промышленностью, гражданским обществом и академическими кругами, чтобы использовать возможности ИИ в интересах национальной безопасности — и обеспечить безопасность, защищенность и надежность американских инноваций в области ИИ в целом — оно рискует уступить позиции стратегическим конкурентам. Уступка технологического преимущества Соединенных Штатов не только нанесет большой ущерб национальной безопасности Америки, но и подорвет цели внешней политики Соединенных Штатов и подорвет безопасность, права человека и демократические нормы во всем мире.

(g) Установление лидерства в сфере национальной безопасности в области ИИ потребует внесения преднамеренных и значимых изменений в аспекты стратегий, возможностей, инфраструктуры, управления и организации правительства Соединенных Штатов. ИИ, вероятно, повлияет почти на все области, имеющие значение для национальной безопасности, и его использование не может быть отнесено к одному институциональному бункеру. Растущая общность ИИ означает, что многие функции, которые до сих пор выполнялись отдельными индивидуальными инструментами, могут в будущем лучше выполняться системами, которые, по крайней мере частично, полагаются на общие многоцелевые возможности ИИ. Такая интеграция будет успешной только в сочетании с надлежащим образом переработанной организационной и информационной инфраструктурой правительства Соединенных Штатов.

(h) В этих усилиях правительство Соединенных Штатов также должно защищать права человека, гражданские права, гражданские свободы, конфиденциальность и безопасность, а также закладывать основу для стабильного и ответственного международного ландшафта управления ИИ. На протяжении всей своей истории Соединенные Штаты были мировым лидером в формировании проектирования, разработки и использования новых технологий не только для продвижения национальной безопасности, но и для защиты и продвижения демократических ценностей. Правительство Соединенных Штатов должно разработать гарантии для своего использования инструментов ИИ и играть активную роль в управлении глобальными нормами и институтами ИИ. Граница ИИ быстро движется, и правительство Соединенных Штатов должно оставаться в курсе текущих технических разработок, не теряя при этом фокуса на своих руководящих принципах.

(i) Целью настоящего меморандума является стимулирование необходимых изменений в подходе правительства США к политике национальной безопасности в области ИИ. В соответствии с указом президента 14110 он направляет действия по укреплению и защите экосистемы ИИ в США; повышению безопасности, надежности и надежности систем ИИ, разработанных и используемых в США; повышению надлежащего, ответственного и эффективного принятия ИИ правительством США в интересах национальной безопасности; и минимизации нецелевого использования ИИ во всем мире.

Раздел 2. Цели.

Политика правительства Соединенных Штатов заключается в том, что следующие три цели будут определять его деятельность в отношении ИИ и национальной безопасности.

(a) **Во-первых**, Соединенные Штаты должны возглавить мировую разработку безопасного, надежного и заслуживающего доверия ИИ. С этой целью правительство Соединенных Штатов должно — в партнерстве с промышленностью, гражданским обществом и академическими кругами — продвигать и защищать основополагающие возможности по всей территории Соединенных Штатов, которые обеспечивают разработку ИИ. Правительство Соединенных Штатов не может воспринимать как должное непревзойденную динамичность и инновационность экосистемы ИИ в Соединенных Штатах; оно должно активно укреплять ее, гарантируя, что Соединенные Штаты останутся самым привлекательным местом для мировых талантов и домом для самых сложных в мире вычислительных мощностей. Правительство Соединенных Штатов также должно предоставить соответствующие рекомендации по безопасности и защите разработчикам и пользователям ИИ, а также тщательно оценить и помочь снизить риски, которые могут представлять системы ИИ.

(b) **Во-вторых,** правительство Соединенных Штатов должно использовать мощный ИИ с соответствующими мерами безопасности для достижения целей национальной безопасности. Новые возможности ИИ, включая все более универсальные модели, предлагают огромные возможности для укрепления национальной безопасности, но эффективное использование этих систем потребует значительных технических, организационных и политических изменений. Соединенные Штаты должны понимать ограничения ИИ, поскольку они используют преимущества этой технологии, и любое

использование ИИ должно уважать демократические ценности в отношении прозрачности, прав человека, гражданских прав, гражданских свобод, конфиденциальности и безопасности.

(c) **В-третьих,** правительство Соединенных Штатов должно продолжать развивать стабильную и ответственную структуру для продвижения международного управления ИИ, которая способствует безопасной, надежной и заслуживающей доверия разработке и использованию ИИ; управляет рисками ИИ; реализует демократические ценности; уважает права человека, гражданские права, гражданские свободы и конфиденциальность; и способствует получению всемирных выгод от ИИ. Оно должно делать это в сотрудничестве с широким кругом союзников и партнеров. Успех Соединенных Штатов в эпоху ИИ будет измеряться не только превосходством технологий и инноваций Соединенных Штатов, но и лидерством Соединенных Штатов в разработке эффективных глобальных норм и участии в институтах, основанных на международном праве, правах человека, гражданских правах и демократических ценностях.

Раздел 3. Продвижение и обеспечение основополагающих возможностей США в области ИИ.

(a) Для сохранения и расширения преимуществ США в области ИИ политика правительства США направлена на содействие прогрессу, инновациям и конкуренции в области разработки ИИ внутри страны; **защиту экосистемы ИИ США от угроз иностранной разведки**; и управление рисками для безопасности, защищенности и надежности ИИ. Лидерство в ответственной разработке ИИ приносит пользу национальной безопасности США, позволяя приложениям, непосредственно связанным с миссией национальной безопасности, разблокируя экономический рост и избегая стратегических неожиданностей. Технологическое лидерство США также дает глобальные преимущества, позволяя единомышленникам коллективно снижать риски неправомерного использования ИИ и несчастных случаев, предотвращать неконтролируемое распространение цифрового авторитаризма и расставлять приоритеты в жизненно важных исследованиях.

3.1 . Содействие прогрессу, инновациям и конкуренции в разработке ИИ в США.

(a) Конкурентное преимущество США в разработке ИИ будет под угрозой из-за отсутствия согласованных усилий правительства США по содействию и обеспечению внутреннего прогресса ИИ, инноваций и конкуренции. Хотя США извлекли выгоду из форы в области ИИ, конкуренты прилагают все усилия, чтобы наверстать упущенное, определили ИИ как главный стратегический приоритет и вскоре могут выделить ресурсы на исследования и разработки, с которыми разработчики ИИ в США не смогут сравниться без соответствующей поддерживающей политики и действий правительства. Поэтому политика правительства США заключается в усилении инноваций и конкуренции путем укрепления ключевых движущих сил прогресса ИИ, таких как технический талант и вычислительная мощность.

(b) Политика правительства Соединенных Штатов заключается в том, что расширение законных возможностей не граждан, высококвалифицированных в области ИИ и смежных областях, въезжать и работать в Соединенных Штатах является **приоритетом национальной безопасности.** Сегодня непревзойденная индустрия ИИ в Соединенных Штатах в значительной степени опирается на идеи блестящих ученых, инженеров и предпринимателей, которые переехали в Соединенные Штаты в поисках академических, социальных и экономических возможностей. Сохранение и расширение преимуществ талантов Соединенных Штатов требует развития талантов дома и постоянного **привлечения и удержания лучших международных умов**.

(c) В соответствии с этими целями:

(i) На постоянной основе Государственный департамент, **Министерство обороны** (DOD) и Министерство внутренней безопасности (DHS) должны использовать все имеющиеся юридические полномочия для содействия привлечению и быстрому доставке в Соединенные Штаты лиц с соответствующими техническими знаниями, которые могли бы повысить конкурентоспособность Соединенных Штатов **в области ИИ и смежных областях, таких как проектирование и производство полупроводников**. Эти мероприятия должны включать всю необходимую проверку этих лиц и должны соответствовать всем соответствующим мерам по снижению рисков. Эта задача

соответствует и дополняет задачи по привлечению талантов в области ИИ в разделе 5 Указа 14110.

(ii) В течение **180 дней** с даты настоящего меморандума председатель Совета экономических консультантов должен подготовить **анализ рынка талантов в сфере ИИ** в Соединенных Штатах и **за рубежом** в той мере, в какой доступны надежные данные.

(iii) В течение 180 дней с даты настоящего меморандума **помощник президента по экономической политике** и директор Национального экономического совета должны координировать экономическую оценку относительного конкурентного преимущества экосистемы ИИ частного сектора США, ключевых источников конкурентного преимущества частного сектора США и возможных рисков для этой позиции, а также должны рекомендовать политику для их смягчения. Оценка может включать в себя такие области, как

(1) проектирование, производство и упаковка чипов, критически важных для деятельности, связанной с ИИ;
(2) доступность капитала;
(3) доступность высококвалифицированных работников в областях, связанных с ИИ;
(4) вычислительные ресурсы и связанные с ними требования к электроэнергии; и
(5) технологические платформы или институты с необходимым масштабом капитала и ресурсов данных для разработки передовой модели ИИ, а также возможные другие факторы.

(iv) В течение 90 дней с даты настоящего меморандума **помощник президента по вопросам национальной безопасности (APNSA)** созовет соответствующие исполнительные департаменты и агентства (агентства) для изучения мер по расстановке приоритетов и оптимизации административных операций по обработке **для всех заявителей на получение визы, работающих с чувствительными технологиями**. Это поможет оптимизировать обработку высококвалифицированных заявителей в области ИИ и других критических и новых технологий. Эти усилия позволят изучить варианты обеспечения адекватного ресурсного обеспечения таких операций и сужения критериев, которые вызывают запросы на получение безопасного консультативного мнения для таких заявителей, в соответствии с целями национальной безопасности.

(d) Текущая парадигма развития ИИ в значительной степени зависит от вычислительных ресурсов. Чтобы сохранить свое лидерство в области ИИ, США должны продолжать разрабатывать самые сложные в мире полупроводники ИИ и строить самую передовую вычислительную инфраструктуру, предназначенную для ИИ.

(e) В соответствии с этими целями:

(i) Министерство обороны, Министерство энергетики (DOE) (включая национальные лаборатории) и Разведывательное сообщество (IC) при планировании и строительстве или реконструкции вычислительных объектов должны учитывать применимость крупномасштабного ИИ к своей миссии. При необходимости агентства должны проектировать и строить объекты, способные использовать передовой ИИ для соответствующих областей **научных исследований и анализа разведданных.** Эти инвестиции должны соответствовать Стратегии устойчивости федеральных миссий, принятой в Указе 13961 от 7 декабря 2020 года (Управление и интеграция устойчивости федеральных миссий).

(ii) На постоянной основе **Национальный научный фонд (NSF**) должен, в соответствии со своими полномочиями, использовать пилотный проект Национального исследовательского ресурса ИИ (NAIRR) и любые будущие усилия NAIRR по распределению вычислительных ресурсов, данных и других критически важных активов для разработки ИИ среди разнообразных субъектов, которые в противном случае не имели бы доступа к таким возможностям — таких как университеты, некоммерческие организации и независимые исследователи (включая доверенных международных партнеров) — для обеспечения того, чтобы исследования ИИ в Соединенных Штатах оставались конкурентоспособными и инновационными. Эта задача соответствует пилотному проекту NAIRR, назначенному в разделе 5 Указа 14110.

(iii) **В течение 180 дней с даты настоящего меморандума Министерство энергетики должно запустить пилотный проект по оценке производительности и эффективности федеративного ИИ и источников данных для обучения, тонкой настройки и вывода в масштабах передового ИИ.**

(iv) Управление начальника штаба Белого дома в сотрудничестве с Министерством энергетики и другими соответствующими агентствами должно **координировать усилия**

по оптимизации разрешений, одобрений и стимулов для строительства инфраструктуры, поддерживающей ИИ, а также окружающих активов, поддерживающих устойчивую работу этой инфраструктуры, таких как чистая генерация энергии, линии электропередачи и высокопроизводительные оптоволоконные каналы передачи данных. Эти усилия должны включать координацию, сотрудничество, консультации и партнерство с государственными, местными, племенными и территориальными органами власти, по мере необходимости, и должны соответствовать целям Соединенных Штатов по управлению климатическими рисками.

(v) Государственный департамент, Министерство обороны, Министерство энергетики, IC и Министерство торговли (Торговля) должны, в зависимости от обстоятельств и в соответствии с действующим законодательством, использовать существующие полномочия для осуществления государственных инвестиций и **поощрения частных инвестиций** в стратегические внутренние и зарубежные технологии ИИ и смежные области. Эти агентства должны оценить необходимость новых полномочий в целях содействия государственным и частным инвестициям в ИИ и смежные возможности.

3.2. Защита ИИ США от угроз иностранной разведки.

(a) В дополнение к реализации промышленных стратегий, которые поддерживают их соответствующие отрасли ИИ, иностранные государства почти наверняка стремятся получить и повторно использовать плоды инноваций ИИ в Соединенных Штатах для обслуживания своих целей национальной безопасности. Исторически такие конкуренты использовали такие методы, как исследовательское сотрудничество, инвестиционные схемы, внутренние угрозы и продвинутый кибершпионаж, чтобы собирать и использовать научные идеи Соединенных Штатов. Политика правительства Соединенных Штатов заключается в защите промышленности, гражданского общества и академической интеллектуальной собственности ИИ США и связанной с ними инфраструктуры от угроз иностранной разведки, чтобы сохранять лидерство в основополагающих возможностях и, при необходимости, оказывать соответствующую правительственную помощь соответствующим неправительственным организациям.

(б) В соответствии с этими целями:

(i) **В течение 90 дней** с даты настоящего меморандума сотрудники **Совета национальной безопасности (СНБ) и Офис директора национальной разведки (ODNI**) должны рассмотреть приоритеты президента в области разведки и Национальную структуру приоритетов разведки в соответствии с Меморандумом о национальной безопасности № 12 от 12 июля 2022 года (приоритеты президента в области разведки) и представить рекомендации, гарантирующие, что такие приоритеты **улучшат выявление и оценку угроз иностранной разведки для экосистемы искусственного интеллекта США** и тесно связанных с ней вспомогательных секторов, таких как те, которые участвуют в проектировании и производстве полупроводников.

(ii) **В течение 180 дней** с даты настоящего меморандума и на постоянной основе после этого ODNI в координации с DOD, Министерством юстиции (DOJ), Министерством торговли, DOE, DHS и другими элементами IC по мере необходимости должны **определить критические узлы в цепочке поставок ИИ и разработать список наиболее вероятных путей, по которым эти узлы могут быть нарушены или скомпрометированы иностранными субъектами.** На постоянной основе эти агентства должны предпринимать все шаги, соответствующие применимому законодательству, для снижения таких рисков.

(c) Иностранные субъекты могут также пытаться получить интеллектуальную собственность Соединенных Штатов с помощью методов серой зоны, таких как передача технологий и требования локализации данных. Интеллектуальная собственность, связанная с ИИ, часто включает критически важные технические артефакты (CTA), которые существенно снижают затраты на воссоздание, достижение или использование мощных возможностей ИИ. Правительство Соединенных Штатов должно защищаться от этих рисков.

(d) В соответствии с этими целями:

(i) В соответствии с Указом президента 14083 от 15 сентября 2022 года (Обеспечение надлежащего учета меняющихся рисков национальной безопасности Комитетом по иностранным инвестициям в Соединенных Штатах) Комитет по иностранным инвестициям в Соединенных Штатах должен, по мере необходимости, рассмотреть, включает ли охватываемая транзакция доступ иностранного субъекта к

конфиденциальной информации о методах обучения ИИ, усовершенствованиях алгоритмов, достижениях в области аппаратного обеспечения, СТА или других конфиденциальных идеях, которые проливают свет на то, как создавать и эффективно использовать мощные системы ИИ.

3.3. Управление рисками для безопасности, защищенности и надежности ИИ. (a) Текущие и будущие системы ИИ могут представлять значительные риски для безопасности, защищенности и надежности, включая риски, возникающие из-за преднамеренного неправильного использования и несчастных случаев. Во многих технологических областях Соединенные Штаты исторически лидировали в мире не только в плане развития возможностей, но и в разработке тестов, стандартов и норм, лежащих в основе надежного и выгодного глобального внедрения. Подход Соединенных Штатов к ИИ не должен отличаться, и упреждающее создание инфраструктуры тестирования для оценки и смягчения рисков ИИ будет иметь важное значение для реализации положительного потенциала ИИ и сохранения лидерства Соединенных Штатов в области ИИ.

(b) Политика правительства Соединенных Штатов заключается в том, чтобы искать новые технические и политические инструменты, которые решают потенциальные проблемы, создаваемые ИИ. Эти инструменты включают процессы для надежного тестирования применимости моделей ИИ к вредоносным задачам и более глубокое партнерство с учреждениями в промышленности, академических кругах и гражданском обществе, способными продвигать исследования, связанные с безопасностью, защитой и надежностью ИИ.

(c) **Министерство торговли**, действуя через **Институт безопасности ИИ (AISI)** в Национальном институте стандартов и технологий (NIST), будет выступать в качестве основной точки контакта правительства США с разработчиками ИИ из частного сектора для содействия добровольному тестированию безопасности и надежности пограничных моделей ИИ до и после публичного развертывания. В координации с соответствующими агентствами по мере необходимости Министерство торговли должно создать устойчивую возможность для руководства добровольным **несекретным тестированием безопасности перед развертыванием пограничных моделей ИИ от имени правительства США**, включая оценку рисков, связанных с кибербезопасностью, биобезопасностью,

химическим оружием, автономностью систем и другими рисками по мере необходимости (не включая ядерный риск, оценку которого будет проводить Министерство энергетики). Добровольное несекретное тестирование безопасности также должно, по мере необходимости, учитывать риски для прав человека, гражданских прав и гражданских свобод, такие как риски, связанные с конфиденциальностью, дискриминацией и предвзятостью, свободой выражения мнений и безопасностью отдельных лиц и групп. Другие агентства, как указано в подпункте 3.3(f) настоящего раздела, должны создать устойчивые возможности для проведения дополнительных добровольных классифицированных испытаний в соответствующих областях знаний. Директивы, изложенные в настоящем подпункте, соответствуют более широким задачам по безопасности ИИ в разделе 4 Указа 14110 и обеспечивают дополнительную ясность относительно соответствующих ролей и обязанностей агентств.

(d) **Ничто в настоящем подразделе не должно препятствовать агентствам проводить собственные оценки систем ИИ, включая испытания**, проводимые до того, как эти системы будут представлены общественности, в целях оценки пригодности для приобретения и закупки этим агентством. Обязанности AISI не распространяются на оценку систем ИИ для потенциального использования правительством Соединенных Штатов в целях национальной безопасности; эти обязанности лежат на агентствах, рассматривающих такое использование, как указано в подразделе 4.2(e) настоящего меморандума и связанной с ним структуре, описанной в этом подразделе.

(e) В соответствии с этими целями Министерство торговли, действуя через AISI в рамках NIST, предпримет следующие действия для содействия оценке текущих и будущих систем ИИ:

(i) **В течение 180 дней** с даты настоящего меморандума и при условии сотрудничества с частным сектором AISI проведет добровольное **предварительное тестирование по крайней мере двух передовых моделей ИИ** до их публичного развертывания или выпуска для оценки возможностей, которые могут представлять угрозу национальной безопасности. Это тестирование должно оценить возможности моделей по содействию наступательным кибероперациям, ускорению разработки биологического и/или химического оружия, автономному выполнению вредоносного поведения, автоматизации разработки и развертывания других моделей с такими возможностями и возникновению

других рисков, выявленных AISI. AISI должна поделиться отзывами с APNSA, межведомственными партнерами по мере необходимости и соответствующими разработчиками моделей относительно результатов рисков, выявленных в ходе такого тестирования, и любых соответствующих мер по смягчению последствий до развертывания.

(ii) В течение 180 дней с даты настоящего меморандума **AISI выпустит руководство для разработчиков ИИ** о том, как тестировать, оценивать и управлять рисками для безопасности, защищенности и надежности, возникающими в связи с моделями фондов двойного назначения, основываясь на руководящих принципах, выпущенных в соответствии с подпунктом 4.1(a) Указа президента 14110. AISI выпустит руководство по темам, включая:

(A) Как измерить возможности, имеющие отношение к риску того, что модели ИИ могут способствовать разработке биологического и химического оружия или автоматизации наступательных кибероперaций;

(B) Как устранить социальные риски, такие как неправомерное использование моделей для преследования или выдачи себя за других людей;

(C) Как разработать меры по смягчению последствий для предотвращения злонамеренного или ненадлежащего использования моделей;

(D) Как проверить эффективность мер по обеспечению безопасности и защиты; и

(E) Как применять методы управления рисками на протяжении всего жизненного цикла разработки и развертывания (предварительная разработка, разработка и развертывание/выпуск).

(iii) В течение 180 дней с даты настоящего меморандума **AISI,** консультируясь с другими агентствами по мере необходимости, **разработает или рекомендует эталонные тесты** или другие методы оценки возможностей и **ограничений систем ИИ в области науки, математики, генерации кода и общих рассуждений**, а также других категорий деятельности, которые AISI сочтет значимыми для оценки возможностей общего

назначения, которые могут иметь отношение к национальной безопасности и общественной безопасности.

(iv) В случае, если AISI или другое агентство определит, что возможности модели фундамента **двойного назначения** могут быть использованы для нанесения существенного вреда общественной безопасности, AISI будет выступать в качестве основного контактного лица, через которое правительство Соединенных Штатов будет передавать такие выводы и любые связанные с ними рекомендации относительно снижения риска разработчику модели.

(v) В течение 270 дней с даты настоящего меморандума и **не реже одного раза в год** впоследствии **AISI** должна представить Президенту через APNSA и предоставить другим межведомственным партнерам по мере необходимости как минимум **один отчет**, который должен включать следующее:

(A) Краткое изложение результатов оценок безопасности ИИ для передовых моделей ИИ, которые были проведены AISI или предоставлены ей;

(B) Краткое изложение того, считает ли AISI меры по снижению риска необходимыми для решения любых проблем, выявленных в ходе оценок, а также выводы относительно эффективности мер по снижению риска; и

(C) Краткое изложение адекватности научно обоснованных инструментов и методов, используемых для информирования о таких оценках.

(f) В соответствии с этими целями другие агентства, указанные ниже, должны предпринять следующие действия в координации с Министерством торговли, действуя через AISI в рамках NIST, для предоставления секретных отраслевых оценок текущих и будущих систем ИИ для кибер-, ядерных и радиологических рисков:

(i) **Все агентства, которые проводят или финансируют испытания и оценки безопасности систем ИИ, должны предоставить результаты таких оценок AISI в течение 30 дней с момента их завершения** в соответствии с применимыми мерами защиты секретной и контролируемой информации.

(ii) В течение 120 дней с даты настоящего меморандума **Агентство национальной безопасности (АНБ), действуя через свой Центр безопасности ИИ (AISC) и в координации с AISI,** должно разработать возможности для проведения быстрого систематического **секретного тестирования** возможностей моделей ИИ обнаруживать, генерировать и/или усугублять наступательные киберугрозы. Такие тесты должны оценить степень, в которой системы ИИ, в случае их ненадлежащего использования, могут ускорить наступательные кибероперации.

(iii) В течение 120 дней с даты настоящего меморандума **DOE,** действуя в первую очередь через Национальное управление ядерной безопасности (NNSA) и в тесном сотрудничестве с AISI и NSA, должно стремиться к разработке возможностей для **проведения быстрых систематических испытаний способности моделей ИИ создавать или усугублять ядерные и радиологические риски.** Эта инициатива должна включать разработку и поддержание инфраструктуры, способной проводить секретные и несекретные испытания, в том числе с использованием ограниченных данных и соответствующей секретной информации об угрозах. **Эта инициатива также должна включать создание и регулярное обновление автоматизированных оценок, разработку интерфейса для обеспечения возможности руководимого человеком red-teaming и создание технических и юридических инструментов,** необходимых для содействия быстрой и безопасной передаче правительственных, открытых и фирменных моделей Соединенных Штатов на эти объекты. В рамках этой инициативы:

(A) В течение **180 дней** с даты настоящего меморандума DOE должно использовать возможности, описанные в подпункте 3.3(f)(iii) настоящего раздела, для завершения первоначальных **оценок радиологических и ядерных знаний**, возможностей и последствий пограничной модели ИИ не позднее, чем через 30 дней после того, как модель будет предоставлена NNSA **на соответствующем уровне классификации**. Эти оценки должны включать испытания систем ИИ как без существенных модификаций, так и, при необходимости, с тонкой настройкой или другими модификациями, которые могут повысить производительность.

(B) В течение 270 дней с даты настоящего меморандума и не реже одного раза в год после этого DOE должен представить Президенту через APNSA как минимум одну оценку, которая должна включать следующее:

(1) Краткое изложение результатов каждой оценки модели ИИ для радиологического и ядерного риска, описанной в подпункте 3.3(f)(iii)(A) настоящего раздела, которую DOE выполнило за предыдущие 12 месяцев;

(2) Рекомендация относительно того, необходимы ли корректирующие действия для решения любых проблем, выявленных в ходе оценки, включая, помимо прочего, действия, необходимые для достижения и поддержания условий соответствия, необходимых для защиты и предотвращения несанкционированного раскрытия ограниченных данных или другой секретной информации в соответствии с Законом об атомной энергии 1954 года; и

(3) Краткое заявление относительно адекватности научно обоснованных инструментов и методов, используемых для информирования об оценках.

(iv) На постоянной основе Министерство внутренней безопасности, действуя через Агентство по кибербезопасности и безопасности инфраструктуры (CISA), продолжит выполнять свои обязанности в отношении применения руководства AISI, как определено в Меморандуме о национальной безопасности 22 от 30 апреля 2024 года (Безопасность и устойчивость критической инфраструктуры) и разделе 4 Указа президента 14110.

(ж) В соответствии с этими целями и для снижения химических и биологических рисков, которые могут возникнуть в результате ИИ:

(i) Правительство Соединенных Штатов должно провести секретные оценки возможностей современных моделей ИИ создавать или усугублять преднамеренные химические и биологические угрозы. В рамках этой инициативы:

(A) В течение 210 дней с даты настоящего меморандума **DOE, DHS и AISI**, в консультации с DOD и другими соответствующими агентствами, должны координировать **разработку дорожной карты для будущих секретных оценок возможностей усовершенствованных моделей ИИ** создавать или усугублять преднамеренные химические и биологические угрозы, которая будет предоставлена APNSA. Эта дорожная карта должна учитывать объем, масштаб и приоритет секретных оценок; надлежащие гарантии, гарантирующие, что оценки и моделирование не будут неправильно истолкованы как разработка наступательных возможностей; надлежащие гарантии для

тестирования конфиденциальной и/или секретной информации; и устойчивое внедрение методологий оценки.

(B) На постоянной основе DHS будет предоставлять экспертные знания, информацию об угрозах и рисках, а также другую техническую поддержку для оценки осуществимости предлагаемых биологических и химических классифицированных оценок; интерпретировать и контекстуализировать результаты оценок; и консультировать соответствующие агентства о потенциальных мерах по снижению рисков.

(C) В течение 270 дней с даты настоящего меморандума Министерство энергетики должно запустить пилотный проект по предоставлению экспертных знаний, инфраструктуры и объектов, способных проводить секретные испытания в этой области.

(ii) **В течение 240 дней с** даты настоящего меморандума Министерство обороны, Министерство здравоохранения и социальных служб (HHS), Министерство энергетики (включая национальные лаборатории), Министерство национальной безопасности, Национальный научный фонд и другие агентства, занимающиеся разработкой **систем ИИ**, в значительной степени **обученных на биологических и химических данных**, должны, по мере необходимости, поддерживать усилия по использованию высокопроизводительных вычислительных ресурсов и систем ИИ для повышения биобезопасности и биозащиты. Эти усилия должны включать:

(A) Разработка инструментов для скрининга in silico химических и биологических исследований и технологий;

(Б) Создание алгоритмов скрининга синтеза нуклеиновых кислот;

(C) Создание высоконадежных программных основ для новых биотехнологий;

(D) Проверка полных заказов или потоков данных из облачных лабораторий и биолитейных заводов; а также

(E) Разработка стратегий снижения риска, таких как медицинские контрмеры.

(iii) После публикации AISI руководства по биологической и химической безопасности, изложенного в подпункте 3.3(e) настоящего раздела, все агентства, которые непосредственно разрабатывают соответствующие модели ИИ двойного назначения, доступные общественности и прошедшие существенную подготовку по биологическим или химическим данным, должны включить это руководство в практику своих агентств, насколько это целесообразно и осуществимо.

(iv) **В течение 180 дней** с даты настоящего меморандума **NSF в координации с DOD**, Commerce (действующим через AISI в рамках NIST), HHS, DOE, Office of Science and Technology Policy (OSTP) и другими соответствующими агентствами **должен стремиться созвать академические исследовательские институты и научные издательства для разработки добровольных лучших практик и стандартов для публикации вычислительных биологических и химических моделей, наборов данных и подходов, включая те, которые используют ИИ и которые могут способствовать производству знаний, информации, технологий и продуктов,** которые могут быть использованы не по назначению для причинения вреда. Это является продолжением деятельности, описанной в подпунктах 4.4 и 4.7 Указа 14110.

(v) В течение 540 дней с даты настоящего меморандума и с учетом **Политики правительства США по надзору за исследованиями двойного назначения**, вызывающими озабоченность, и патогенами с повышенным пандемическим потенциалом **сотрудники OSTP, NSC** и Управления политики готовности к пандемиям и реагирования на них, в консультации с соответствующими агентствами и внешними заинтересованными сторонами по мере необходимости, **разработают руководство**, пропагандирующее преимущества и снижающее риски, связанные с биологическими и химическими исследованиями in silico .

(h) **Агентства должны предпринять следующие действия для улучшения основополагающего понимания безопасности, защищенности и надежности ИИ:**

(i) Министерство обороны, Министерство торговли, Министерство энергетики, Министерство внутренней безопасности, Министерство обороны США, Национальный научный фонд, Агентство национальной безопасности и Национальное агентство геопространственной разведки (NGA) должны, в зависимости от обстоятельств и в

соответствии с действующим законодательством, **отдавать приоритет исследованиям безопасности и надежности ИИ.** В зависимости от обстоятельств и в соответствии с существующими органами власти они должны **стремиться к партнерству с ведущими государственными, промышленными, гражданскими, академическими и другими учреждениями, имеющими опыт в этих областях**, с целью ускорения технического и социально-технического прогресса в области безопасности и надежности ИИ. Эта работа может включать исследования интерпретируемости, формальных методов, технологий повышения конфиденциальности, методов устранения рисков для гражданских свобод и прав человека, взаимодействия человека и ИИ и/или социально-технических последствий обнаружения и маркировки синтетического и аутентичного контента (например, для решения проблемы злонамеренного использования ИИ для создания вводящих в заблуждение видеороликов или изображений, в том числе стратегически вредоносного или несогласованного интимного характера, политических или общественных деятелей).

(ii) Министерство обороны, Министерство торговли, Министерство энергетики, Министерство внутренней безопасности, Министерство национальной безопасности, Национальный фонд национальной безопасности и Агентство национальной безопасности должны, в зависимости от обстоятельств и в соответствии с действующим законодательством, **отдавать приоритет исследованиям по улучшению безопасности, надежности и устойчивости систем и средств управления ИИ**. Эти организации должны, в зависимости от обстоятельств и в соответствии с действующим законодательством, сотрудничать с другими агентствами, промышленностью, гражданским обществом и академическими кругами. В соответствующих случаях Министерство обороны, Министерство внутренней безопасности (действуя через CISA), Федеральное бюро расследований и Агентство национальной безопасности (действуя через AISC) должны публиковать несекретные руководства, касающиеся известных уязвимостей и угроз кибербезопасности ИИ; передовой опыт по предотвращению, обнаружению и смягчению таких проблем во время обучения и развертывания моделей; и интеграцию ИИ в другие программные системы. Эта работа должна включать изучение роли и уязвимостей, потенциально вызванных системами ИИ, используемыми в критической инфраструктуре.

(i) Агентства должны принять меры по защите секретной и контролируемой информации, учитывая потенциальные риски, связанные с ИИ:

(i) В ходе регулярных обновлений политик и процедур Министерство обороны, Министерство энергетики и СК должны учитывать, как анализ, обеспечиваемый инструментами ИИ, может повлиять на решения, связанные с рассекречиванием материалов, стандартами достаточной анонимности и аналогичными действиями, а также на надежность существующих оперативных мер безопасности и контроля справедливости для защиты секретной или контролируемой информации, учитывая, что системы ИИ продемонстрировали способность извлекать ранее недоступную информацию из отредактированных и анонимизированных данных.

Раздел 4. Ответственное использование ИИ для достижения целей национальной безопасности.

(a) Политика правительства Соединенных Штатов заключается в том, чтобы действовать решительно, чтобы обеспечить эффективное и ответственное использование ИИ для содействия своей миссии национальной безопасности. Достижение мирового лидерства в применении ИИ в целях национальной безопасности потребует эффективного партнерства с организациями за пределами правительства, а также значительной внутренней трансформации, включая укрепление эффективных функций надзора и управления.

4.1. Обеспечение эффективного и ответственного использования ИИ.

(a) Политика правительства Соединенных Штатов заключается в адаптации своих партнерств, политик и инфраструктуры для использования возможностей ИИ надлежащим образом, эффективно и ответственно. Эти изменения должны сбалансировать уникальные потребности каждого агентства в надзоре, данных и приложениях с существенными преимуществами, связанными с совместным использованием мощных ресурсов ИИ и вычислений в рамках правительства Соединенных Штатов. Изменения также должны основываться на четком **понимании сравнительных преимуществ правительства Соединенных Штатов по отношению к промышленности, гражданскому обществу и академическим кругам** и должны использовать предложения от внешних соавторов и подрядчиков по мере необходимости. **Правительство Соединенных Штатов должно максимально использовать богатую экосистему ИИ Соединенных Штатов**, стимулируя инновации в области безопасного,

надежного и заслуживающего доверия ИИ и поощряя отраслевую конкуренцию при выборе подрядчиков, получателей грантов и исследовательских соавторов. Наконец, правительство Соединенных Штатов должно учитывать важные технические и политические соображения таким образом, чтобы обеспечить целостность и совместимость, необходимые для достижения его целей, одновременно защищая права человека, гражданские права, гражданские свободы, конфиденциальность и безопасность.

(б) Правительству Соединенных Штатов необходим **обновленный набор общегосударственных процедур для привлечения, найма, развития и удержания специалистов** в области ИИ и специалистов по ИИ в целях обеспечения национальной безопасности.

(c) В соответствии с этими целями:

(i) В ходе регулярных обзоров правовых, политических и нормативно-правовых рамок Государственный департамент, DOD, DOJ, DOE, DHS и IC должны пересматривать, по мере необходимости, свою политику найма и удержания и стратегии для ускорения ответственного принятия ИИ. Агентства должны **учитывать потребности в технических талантах, необходимых для принятия ИИ**, и интегрировать его в свои миссии и другие роли, необходимые для эффективного использования ИИ, такие как управление, этика и политические позиции, связанные с ИИ. Эти политики и стратегии должны определять финансовые, организационные и связанные с безопасностью препятствия, а также потенциальные меры по смягчению последствий в соответствии с действующим законодательством. Такие меры должны также включать рассмотрение программ по привлечению экспертов с соответствующей технической экспертизой из промышленности, академических кругов и гражданского общества, включая стипендии для программ обслуживания, и аналогичные инициативы, которые будут знакомить государственных служащих с соответствующими неправительственными организациями таким образом, чтобы формировать техническое, организационное и культурное знакомство с отраслью ИИ. Эти политики и стратегии должны использовать все доступные полномочия, включая **ускоренные процедуры допуска к секретной информации, в зависимости от обстоятельств, для устранения нехватки талантов, связанных с ИИ, в правительстве**.

(ii) В течение 120 дней с даты настоящего меморандума Государственный департамент, Министерство обороны, Министерство юстиции, Министерство энергетики, Министерство внутренней безопасности и IC должны, по согласованию с Управлением по управлению и бюджету (OMB), определить возможности обучения и подготовки для повышения компетентности своих сотрудников в области искусственного интеллекта посредством инициатив, которые могут включать **обучение и найм на основе навыков**.

(d) Для ускорения использования ИИ в интересах своей национальной безопасности правительству Соединенных Штатов нужны скоординированные **и эффективные системы закупок.** Это потребует расширенного потенциала для оценки, определения и формулирования требований, связанных с ИИ, в целях национальной безопасности, а также **улучшенной доступности для компаний ИИ, у которых нет значительного предыдущего опыта работы с правительством Соединенных Штатов**.

(e) В соответствии с этими целями:

(i) **В течение 30 дней** с даты настоящего меморандума, DOD и ODNI, в координации с OMB и другими агентствами по мере необходимости, **создадут рабочую группу для решения вопросов, связанных с закупкой ИИ** элементами DOD и IC и для использования на NSS. По мере необходимости, рабочая группа будет консультироваться с директором NSA, как с национальным менеджером по NSS, при разработке рекомендаций по приобретению и закупке ИИ для использования на NSS.

(ii) В течение 210 дней с даты настоящего меморандума рабочая группа, описанная в подпункте 4.1(e)(i) настоящего раздела, должна предоставить письменные рекомендации Федеральному совету по регулированию закупок (FARC) относительно изменений в существующих правилах и руководствах, в зависимости от обстоятельств и в соответствии с действующим законодательством, для содействия достижению следующих целей в отношении ИИ, закупаемого подразделениями Министерства обороны и IC и для использования в NSS:

(A) **Обеспечение объективных показателей для измерения и повышения безопасности, защищенности и надежности систем ИИ**;

(B) Ускорение процесса приобретения и закупки ИИ в соответствии с Положением о федеральных закупках при одновременном проведении соответствующих проверок для снижения рисков безопасности;

(C) Упрощение процессов таким образом, чтобы компании, не имеющие опытных команд по заключению контрактов, могли осмысленно конкурировать за соответствующие контракты, чтобы гарантировать правительству Соединенных Штатов доступ к широкому спектру систем ИИ и конкурентоспособность рынка ИИ;

(D) Структурирование конкурсов для поощрения активного участия и достижения максимальной выгоды для правительства, например, путем включения требований, способствующих совместимости, и уделения приоритетного внимания техническим возможностям поставщиков при оценке предложений;

(E) Обеспечение совместного использования ИИ в максимально возможной степени и по мере необходимости в соответствующих учреждениях; и

(F) Обеспечение того, чтобы учреждения с особыми полномочиями и задачами могли реализовывать другие политики, когда это уместно и необходимо.

(iii) FARC, по мере необходимости и в соответствии с действующим законодательством, рассмотрит возможность внесения поправок в Положение о федеральных закупках с целью кодификации рекомендаций, предоставленных рабочей группой в соответствии с подпунктом 4.1(e)(ii) настоящего раздела, которые могут иметь общеправительственное применение.

(iv) Министерство обороны и Министерство национальной безопасности США будут стремиться к постоянному взаимодействию с различными заинтересованными сторонами из частного сектора США, включая компании, занимающиеся технологиями искусственного интеллекта и обороной, а также членов инвестиционного сообщества США, с целью выявления и лучшего понимания новых возможностей, которые могут принести пользу или иным образом повлиять на миссию США по обеспечению национальной безопасности.

(f) Правительству Соединенных Штатов необходимы **четкие, модернизированные и надежные политики и процедуры,** которые позволят быстро разрабатывать и использовать ИИ в целях национальной безопасности в соответствии с правами человека, гражданскими правами, гражданскими свободами, конфиденциальностью, безопасностью и другими демократическими ценностями.

(ж) В соответствии с этими целями:

(i) Министерство обороны и МК должны, по мере необходимости, консультируясь с Министерством юстиции, пересмотреть свои соответствующие правовые, политические, гражданские свободы, конфиденциальность и рамки соответствия, включая международно-правовые обязательства, и, по мере необходимости и в соответствии с действующим законодательством, стремиться разрабатывать или пересматривать политику и процедуры, позволяющие эффективно и ответственно использовать ИИ, принимая во внимание следующее:

(A) Вопросы, возникающие в связи **с приобретением, использованием, хранением, распространением и утилизацией моделей,** обученных на наборах данных, которые включают персональную информацию, прослеживаемую до конкретных лиц Соединенных Штатов, общедоступную информацию, коммерчески доступную информацию и интеллектуальную собственность, в соответствии с разделом 9 Указа президента 14110;

(B) **Руководство, которое должно быть разработано Министерством юстиции в консультации с Министерством обороны и Управлением национальной разведки** в отношении конституционных соображений, возникающих в связи с приобретением и использованием ИИ Международным разведывательным управлением;

(C) **Проблемы, связанные с классификацией и разделением на категории**;

(D) **Алгоритмическая предвзятость, непоследовательная работа, неточные выходные данные и другие известные виды сбоев ИИ**;

(E) **Угрозы аналитической целостности при использовании инструментов ИИ**;

(F) Риски, возникающие из-за отсутствия гарантий защиты прав человека, гражданских прав, гражданских свобод, частной жизни и других демократических ценностей, как более подробно рассматривается в подразделе 4.2 настоящего раздела;

(G) **Препятствия к обмену моделями ИИ и связанными с ними знаниями с союзниками и партнерами; а также**

(H) Возможные несоответствия между использованием ИИ и выполнением международных правовых обязательств и обязанностей.

(ii) В зависимости от ситуации, политики, описанные в подпункте 4.1(g) настоящего раздела, должны соответствовать указаниям Комитета по национальной безопасности и Министерства обороны, регулирующим безопасность ИИ, используемого в системе национальной безопасности, политикам Директора национальной разведки, регулирующим принятие ИИ Международным разведывательным управлением, и указаниям Административно-бюджетного управления, регулирующим безопасность ИИ, используемого в системах, не относящихся к системе национальной безопасности.

(iii) На постоянной основе каждое агентство, использующее ИИ в НСС, должно, по согласованию с ODNI и DOD, предпринимать все необходимые и соответствующие применимому законодательству шаги для ускорения ответственного утверждения систем ИИ для использования в НСС и **аккредитации НСС, использующих системы ИИ**.

(h) *Сеть союзников и партнеров Соединенных Штатов дает значительные преимущества перед конкурентами*. В соответствии со Стратегией национальной безопасности 2022 года или любыми последующими стратегиями правительство Соединенных Штатов должно инвестировать и активно **обеспечивать совместную разработку и совместное развертывание возможностей ИИ с избранными союзниками и партнерами.**

(i) В соответствии с этими целями:

(i) **В течение 150 дней** с даты настоящего меморандума Министерство обороны в координации с Государственным департаментом и ODNI оценит возможность продвижения, увеличения и продвижения совместной разработки и совместного

использования ИИ и активов с поддержкой ИИ с избранными союзниками и партнерами. Эта оценка должна включать:

(A) **Потенциальный список иностранных государств, с которыми такая совместная разработка или совместное развертывание могут быть осуществимы**;

(B) Список двусторонних и многосторонних форумов для потенциального взаимодействия;

(C) Потенциальные **концепции совместной разработки** и совместного развертывания;

(D) Предлагаемые соответствующие классификации испытательные транспортные средства для совместно разрабатываемых возможностей ИИ; и

(E) Соображения относительно **существующих программ**, соглашений или договоренностей, которые можно использовать в качестве основы для будущей совместной разработки и совместного развертывания возможностей ИИ.

(j) Правительству Соединенных Штатов необходимо улучшить внутреннюю координацию в отношении использования и подхода к ИИ в национальной системе безопасности, чтобы обеспечить совместимость и совместное использование ресурсов в соответствии с действующим законодательством, а также воспользоваться преимуществами универсальности и экономии за счет масштаба, которые обеспечивают передовые модели ИИ.

(k) В соответствии с этими целями:

(i) На постоянной основе DOD и ODNI должны выпускать или пересматривать соответствующие **руководящие принципы для улучшения консолидации и взаимодействия между функциями ИИ в NSS**. Эти руководящие принципы должны быть направлены на обеспечение того, чтобы правительство Соединенных Штатов могло эффективно координировать и совместно использовать ресурсы, связанные с ИИ, в соответствии с применимым законодательством. Такая работа должна включать:

(A) **Рекомендация организационных практик агентств для улучшения исследований и внедрения ИИ, охватывающих несколько учреждений национальной безопасности**. Чтобы поощрять принятие ИИ в целях национальной безопасности, эти меры должны быть направлены на создание максимально возможной согласованности в пересмотренных практиках.

(B) Меры, которые позволяют консолидировать исследования, разработки и закупки для систем искусственного интеллекта общего назначения и поддерживающей инфраструктуры, **чтобы несколько агентств могли совместно использовать эти инструменты** в объеме, соответствующем применимому законодательству, при этом обеспечивая надлежащий контроль за конфиденциальными данными.

(C) Согласование политик и процедур национальной безопасности, связанных с ИИ, между агентствами, насколько это практически осуществимо и целесообразно, а также соответствует применимому законодательству.

(D) Разработка политик и процедур, соответствующих применимому законодательству, для обмена информацией между Министерством обороны и IC в случаях, когда система ИИ, разработанная, развернутая или используемая подрядчиком, демонстрирует риски, связанные с безопасностью, защитой и надежностью, в том числе с правами человека, гражданскими правами, гражданскими свободами или конфиденциальностью.

4.2. Укрепление управления ИИ и управления рисками.

(a) Поскольку правительство Соединенных Штатов быстро переходит к принятию ИИ в поддержку своей миссии по обеспечению национальной безопасности, оно должно продолжать предпринимать активные шаги для защиты прав человека, гражданских прав, гражданских свобод, конфиденциальности и безопасности; **гарантировать, что ИИ используется в соответствии с полномочиями президента как главнокомандующего, чтобы решать, когда отдавать приказы о военных операциях в целях обороны страны; и гарантировать, что военное использование возможностей ИИ является подотчетным, в том числе посредством такого использования во время военных операций в рамках ответственной человеческой цепочки командования и контроля**.

Соответственно, правительство Соединенных Штатов должно разработать и внедрить надежные методы управления ИИ и управления рисками, чтобы гарантировать, что его инновации в области ИИ соответствуют демократическим ценностям, обновляя политические рекомендации при необходимости. В свете разнообразных полномочий и миссий в охватываемых агентствах с миссией по обеспечению национальной безопасности и быстрых темпов текущих технологических изменений такие структуры управления ИИ и управления рисками должны:

(i) **структурированы** в той мере, в какой это допускается законом, таким образом, чтобы они могли адаптироваться к будущим возможностям и рискам, связанным с новыми техническими разработками;

(ii) настолько **единообразны** во всех учреждениях, насколько это практически осуществимо и целесообразно, чтобы обеспечить взаимодействие, при соблюдении уникальных полномочий и миссий;

(iii) Разработаны для **обеспечения инноваций**, способствующих достижению целей национальной безопасности Соединенных Штатов;

(iv) быть настолько **прозрачным для общественности**, насколько это практически осуществимо и целесообразно, при одновременной защите секретной или контролируемой информации;

(v) разрабатываться и применяться таким образом и с использованием средств, позволяющих **интегрировать защиту, контроль и гарантии** прав человека, гражданских прав, гражданских свобод, конфиденциальности и безопасности, где это уместно; и

(vi) Разработано с целью **отразить лидерство Соединенных Штатов** в обеспечении широкой международной поддержки правил и норм, которые подкрепляют подход Соединенных Штатов к управлению ИИ и управлению рисками.

(b) Охваченные агентства должны разрабатывать и использовать ИИ ответственно, в соответствии с законодательством и политикой Соединенных Штатов, демократическими ценностями, а также международными правовыми и договорными обязательствами, включая международное гуманитарное право и право прав человека. Все должностные

лица агентств сохраняют свои существующие полномочия и обязанности, установленные в других законах и политиках.

(c) В соответствии с этими целями:

(i) Руководители охваченных агентств должны, в соответствии со своими полномочиями, контролировать, оценивать и смягчать риски, напрямую связанные с разработкой и использованием ИИ их агентством. Такие риски могут возникать из-за зависимости от результатов ИИ для информирования, влияния, принятия решений или исполнения решений или действий агентства при использовании в контексте обороны, разведки или обеспечения правопорядка и могут влиять на права человека, гражданские права, гражданские свободы, конфиденциальность, безопасность, национальную безопасность и демократические ценности. Эти риски от использования ИИ включают следующее:

(A) **Риски для физической безопасности**: использование ИИ может представлять непреднамеренный риск для жизни или имущества человека.

(B) **Ущерб конфиденциальности:** проектирование, разработка и эксплуатация ИИ могут привести к причинению вреда, смущению, несправедливости и предвзятости по отношению к отдельным лицам.

(C) **Дискриминация и предвзятость**: использование ИИ может привести к незаконной дискриминации и пагубной предвзятости, что может привести, например, к ненадлежащему наблюдению и профилированию, а также к другим видам вреда.

(D) **Ненадлежащее использование**: операторы, использующие системы ИИ, могут не полностью понимать возможности и ограничения этих технологий, включая системы, используемые в конфликтах. Такое незнание может повлиять на способность операторов применять соответствующие уровни человеческого суждения.

(E) **Отсутствие прозрачности:** у агентств могут быть пробелы в документации по разработке и использованию ИИ, а у общественности может отсутствовать доступ к информации о том, как ИИ используется в контексте национальной безопасности, из-за необходимости защиты секретной или контролируемой информации.

(F) **Отсутствие ответственности**: программы обучения и руководства для персонала агентства по правильному использованию систем ИИ могут быть недостаточными, в том числе для снижения риска чрезмерной зависимости от систем ИИ (например, «автоматизированной предвзятости»), а механизмы ответственности могут неадекватно реагировать на возможное преднамеренное или небрежное неправомерное использование технологий на базе ИИ.

(G) **Утечка данных**: системы ИИ могут раскрывать аспекты своих обучающих данных — как непреднамеренно, так и в результате преднамеренной манипуляции со стороны злоумышленников — а утечка данных может возникнуть в результате обучения систем ИИ на основе секретной или контролируемой информации при использовании в сетях, где такая информация не допускается.

(H) **Низкая производительность**: системы ИИ, которые неправильно или недостаточно обучены, используются для целей, выходящих за рамки их обучающего набора, или неправильно интегрированы в рабочие процессы человека, могут демонстрировать низкую производительность, в том числе способами, которые приводят к **непоследовательным результатам** или незаконной дискриминации и пагубным предубеждениям, или которые **подрывают целостность процессов принятия решений**.

(I) **Преднамеренное манипулирование** и неправомерное использование: иностранные конкуренты и злоумышленники могут преднамеренно подрывать точность и эффективность систем ИИ или пытаться извлечь конфиденциальную информацию из таких систем.

(d) Политика правительства Соединенных Штатов в области управления ИИ и управления рисками должна идти в ногу с развитием технологий.

(e) В соответствии с этими целями:

(i) Структура ИИ под названием **«Структура по развитию управления ИИ и управления рисками в сфере национальной безопасности»** (Структура ИИ) должна далее реализовывать этот подраздел. Структура ИИ должна быть одобрена Комитетом заместителей СНБ в рамках процесса, описанного в Меморандуме 2 по национальной безопасности от 4 февраля 2021 г. (Обновление системы Совета национальной

безопасности) или в любом последующем процессе и должна периодически пересматриваться в рамках этого процесса. Этот процесс должен определить, необходимы ли корректировки для устранения рисков, указанных в подпункте 4.2(c) настоящего раздела, и других тем, охватываемых Структурой ИИ. Структура ИИ должна служить ориентированным на национальную безопасность аналогом Меморандума OMB M-24-10 от 28 марта 2024 г. (Развитие управления, инноваций и управления рисками для использования искусственного интеллекта агентством) и любых последующих политик OMB. В той степени, в которой это осуществимо, целесообразно и соответствует применимому законодательству, Структура ИИ должна быть максимально согласована с этими политиками OMB и должна быть обнародована.

(ii) Структура ИИ, описанная в подпункте 4.2(e)(i) настоящего раздела, и любой последующий документ должны, как минимум, и в той мере, в которой это соответствует применимому законодательству, указывать следующее:

(A) **Каждое охваченное агентство должно иметь главного должностного лица по искусственному интеллекту**, которое несет основную ответственность в этом агентстве, совместно с другими ответственными должностными лицами, за управление использованием ИИ агентством, продвижение инноваций в области ИИ в агентстве и управление рисками, связанными с использованием ИИ агентством, в соответствии с подпунктом 3(b) Меморандума OMB M-24-10, насколько это практически осуществимо.

(B) Охваченные агентства должны иметь **Советы по управлению ИИ** для координации и управления вопросами ИИ через соответствующих старших руководителей агентства.

(C) Руководство по видам деятельности ИИ, которые представляют неприемлемый уровень риска и должны быть запрещены.

(D) Руководство по видам деятельности ИИ, которые оказывают «высокое воздействие» и требуют минимальных методов управления рисками, включая использование ИИ с высоким воздействием, которое затрагивает персонал правительства Соединенных Штатов. Такие виды деятельности с высоким воздействием должны включать ИИ, выходные данные которого служат принципиальной основой для решения или действия, которые могут усугубить или создать значительные риски для национальной безопасности, международных норм, прав человека, гражданских прав, гражданских свобод,

конфиденциальности, безопасности или других демократических ценностей. Минимальные методы управления рисками для ИИ с высоким воздействием должны включать механизм для агентств по оценке ожидаемых преимуществ и потенциальных рисков ИИ; механизм оценки качества данных; достаточные методы тестирования и оценки; смягчение незаконной дискриминации и пагубных предубеждений; требования к обучению, оценке и надзору за людьми; постоянный мониторинг; и дополнительные гарантии для военнослужащих, федеральных гражданских служащих и лиц, которые получают предложение о трудоустройстве от охваченного агентства.

(E) Охваченные агентства должны гарантировать, что должностные лица по вопросам конфиденциальности, гражданских свобод и безопасности будут интегрированы в структуры управления и надзора за ИИ. Такие должностные лица должны сообщать о результатах главам агентств и должностным лицам по надзору, по мере необходимости, используя существующие каналы отчетности, когда это возможно.

(F) Охваченные агентства должны обеспечить наличие достаточных программ обучения, руководств и процессов подотчетности для обеспечения надлежащего использования систем ИИ.

(G) Охваченные агентства должны вести **ежегодную инвентаризацию своих высокоэффективных систем ИИ** и использования ИИ и предоставлять обновленную информацию по этому инвентарю руководителям агентств и APNSA.

(H) Охваченные агентства должны гарантировать, что защита осведомителей достаточна для решения проблем, которые могут возникнуть при разработке и использовании ИИ и систем ИИ.

(I) Охваченные агентства должны разработать и внедрить **процедуры отказа от высокоэффективного использования ИИ,** которые обеспечивают баланс между надежной реализацией мер по снижению рисков, предусмотренных в настоящем меморандуме и Рамочной программе ИИ, и необходимостью использования ИИ для сохранения и продвижения критически важных миссий и операций агентства.

(J) Охваченные агентства должны **внедрить руководство по кибербезопасности** или указания, связанные с системами ИИ, выпущенные Национальным менеджером по NSS,

для снижения рисков, создаваемых злоумышленниками, использующими новые технологии, и для обеспечения взаимодействия ИИ между агентствами. В течение 150 дней с даты настоящего меморандума и периодически после этого Национальный менеджер по NSS должен выпустить минимальное руководство по кибербезопасности и/или указания для ИИ, используемого в качестве компонента NSS, которые должны быть включены в руководство по управлению ИИ, подробно изложенное в подпункте 4.2(g)(i) настоящего раздела.

(f) **Правительству Соединенных Штатов необходимо конкретное руководство относительно использования ИИ в национальной системе безопасности**.

(ж) В соответствии с этими целями:

(i) **В течение 180 дней** с даты настоящего меморандума главы Государственного департамента, Министерства финансов, Министерства обороны, Министерства юстиции, Министерства торговли, Министерства энергетики, Министерства внутренней безопасности, ODNI (действующего от имени 18 элементов IC) и любого другого охваченного агентства, которое использует ИИ как часть NSS (главы департаментов), должны **выпустить или обновить руководство для своих компонентов/подведомственных агентств по управлению ИИ и управлению рисками для NSS**, согласующееся с политиками в этом подразделе, Системой ИИ и другими применимыми политиками. Главы департаментов должны ежегодно пересматривать свои соответствующие руководства и обновлять такие руководства по мере необходимости. Это руководство и любые его обновления должны быть предоставлены APNSA до выпуска. Это руководство должно быть несекретным и должно быть доступно общественности в той степени, в которой это осуществимо и целесообразно, хотя оно может иметь секретное приложение. Главы департаментов должны стремиться к гармонизации своих руководств, а APNSA должна созывать межведомственное совещание не реже одного раза в год с целью гармонизации руководств глав департаментов по управлению ИИ и управлению рисками в той степени, в которой это осуществимо и целесообразно, с учетом различных полномочий и миссий агентств.

Гармонизация должна осуществляться в следующих областях:

(A) Внедрение методов управления рисками для высокоэффективных ИИ;

(B) стандарты и мероприятия в области искусственного интеллекта и систем искусственного интеллекта, в том числе касающиеся обучения, тестирования, аккредитации, безопасности и кибербезопасности; а также

(C) Любые другие проблемы, влияющие на взаимодействие ИИ и систем ИИ.

Раздел 5. Создание стабильного, ответственного и глобально выгодного ландшафта международного управления ИИ.

(a) На протяжении всей своей истории Соединенные Штаты играли важную роль в формировании международного порядка, обеспечивающего безопасное, надежное и заслуживающее доверия глобальное внедрение новых технологий, а также защиту демократических ценностей. Эти вклады варьировались от установления режимов нераспространения биологического, химического и ядерного оружия до создания основ для многостороннего управления Интернетом. Как и эти прецеденты, ИИ потребует **новых глобальных норм и механизмов координации**, в разработке которых правительство Соединенных Штатов должно поддерживать активную роль.

(b) Политика правительства Соединенных Штатов заключается в том, что международное участие Соединенных Штатов в области ИИ должно поддерживать и способствовать улучшению безопасности, защищенности и надежности систем ИИ во всем мире; продвигать демократические ценности, включая уважение прав человека, гражданских прав, гражданских свобод, конфиденциальности и безопасности; предотвращать неправомерное использование ИИ в контексте национальной безопасности; и содействовать равноправному доступу к преимуществам ИИ. Правительство Соединенных Штатов должно продвигать международные соглашения, сотрудничество и другие существенные и нормотворческие инициативы в соответствии с этой политикой.

(c) В соответствии с этими целями:

(i) **В течение 120 дней** с даты настоящего меморандума Государственный департамент в координации с Министерством обороны, Министерством торговли, Министерством внутренней безопасности, Миссией США при Организации Объединенных Наций (USUN) и Агентством США по международному развитию (USAID) должен разработать

Стратегию по продвижению международных норм управления ИИ в соответствии с безопасным, надежным и заслуживающим доверия ИИ и демократическими ценностями, включая права человека, гражданские права, гражданские свободы и конфиденциальность. Эта стратегия должна охватывать двустороннее и многостороннее взаимодействие и отношения с союзниками и партнерами. Она также должна включать руководство по взаимодействию с конкурентами и должна описывать подход к работе в международных институтах, таких как Организация Объединенных Наций и Группа 7 (G7), а также технические организации. Стратегия должна:

(A) **Разрабатывать и продвигать общие на международном уровне определения, нормы, ожидания и стандарты**, соответствующие политике Соединенных Штатов и существующим усилиям, которые будут способствовать безопасной, надежной и заслуживающей доверия разработке и использованию ИИ во всем мире. Эти нормы должны быть максимально согласованы с внутренним управлением ИИ Соединенных Штатов (включая Указ президента 14110 и Меморандум OMB M-24-10), Международным кодексом поведения для организаций, разрабатывающих передовые системы ИИ, выпущенным G7 в октябре 2023 года, Принципами Организации экономического сотрудничества и развития в отношении ИИ, Резолюцией Генеральной Ассамблеи Организации Объединенных Наций A/78/L.49 и другими соответствующими международными рамками, поддерживаемыми Соединенными Штатами (такими как Политическая декларация об ответственном военном использовании ИИ и автономии) и инструментами. Препятствуя ненадлежащему использованию и поощряя соответствующие гарантии, эти нормы и стандарты должны быть направлены на снижение вероятности того, что ИИ причинит вред или окажет неблагоприятное воздействие на права человека, демократию или верховенство закона.

(B) **Содействовать ответственному и этичному использованию ИИ** в контексте национальной безопасности в соответствии с демократическими ценностями и в соответствии с применимым международным правом. Стратегия должна продвигать нормы и практику, установленные настоящим меморандумом, и меры, одобренные в Политической декларации об ответственном военном использовании ИИ и автономии.

Раздел 6. Обеспечение эффективной координации, исполнения и отчетности по политике ИИ.

(a) Правительство Соединенных Штатов должно работать в тесной координации, чтобы добиться прогресса в эффективном и ответственном принятии ИИ. **Учитывая скорость, с которой развиваются технологии ИИ, правительство Соединенных Штатов должно быстро учиться, адаптироваться к новым стратегическим разработкам, внедрять новые возможности и противостоять новым рискам.**

(б) В соответствии с этими целями:

(i) **В течение 270 дней** с даты настоящего меморандума и **ежегодно в течение как минимум следующих 5 лет** главы Государственного департамента, Министерства обороны, Министерства торговли, Министерства энергетики, ODNI (действующего от имени IC), USUN и USAID должны **представить Президенту через APNSA отчет, содержащий подробный отчет об их деятельности в ответ на их задачи во всех разделах настоящего меморандума, включая секретное приложение к настоящему меморандуму**, и содержащий план дальнейших действий. Центральное разведывательное управление (ЦРУ), АНБ, Управление военной разведки (DIA) и NGA должны представить отчеты о своей деятельности в ODNI для включения в полном объеме в качестве приложения к отчету ODNI относительно деятельности IC. NGA, АНБ и DIA также должны представить свои отчеты в DOD для включения в полном объеме в качестве приложения к отчету DOD.

(ii) **В течение 45 дней** с даты настоящего меморандума главные должностные лица по искусственному интеллекту Государственного департамента, Министерства обороны, Министерства юстиции, Министерства энергетики, Министерства внутренней безопасности, Административно-бюджетного управления, ODNI, ЦРУ, Разведывательного управления, Агентства национальной безопасности и Национального агентства по безопасности, а также соответствующий технический персонал сформируют **Координационную группу по искусственному интеллекту в области национальной безопасности (Координационная группа**). Любой главный должностной сотрудник по искусственному интеллекту агентства, являющегося членом Комитета по системам национальной безопасности, может также присоединиться к Координационной группе в

качестве полноправного члена. Координационная группа будет работать под сопредседательством главных должностных лиц по искусственному интеллекту ODNI и Министерства обороны. Координационная группа рассмотрит способы гармонизации политик, касающихся разработки, аккредитации, приобретения, использования и оценки искусственного интеллекта в области национальной безопасности. Эта работа может включать разработку:

(A) **Улучшение обучения** и осведомленности для обеспечения того, чтобы агентства отдавали приоритет наиболее эффективным системам ИИ, ответственно разрабатывали и использовали ИИ, а также эффективно оценивали системы ИИ;

(B) **Передовой опыт** по выявлению и снижению рисков, связанных с иностранной разведкой, и соображений прав человека, связанных с закупками ИИ;

(C) **Передовая практика** по обеспечению взаимодействия между развертываниями ИИ в агентствах, включая соглашения о взаимодействии данных и обмене данными, в зависимости от обстоятельств и в соответствии с действующим законодательством;

(D) Процесс поддержания, обновления и **распространения таких тренингов и передового опыта на постоянной основе;**

(E) политические инициативы, связанные с ИИ, направленные на устранение пробелов в регулировании, возникающих в процессе разработки политики в масштабах всей исполнительной власти; и

(F) Гибкий процесс для увеличения скорости приобретения, проверки и предоставления возможностей ИИ в соответствии с действующим законодательством.

(iii) **В течение 90 дней** с даты настоящего меморандума Координационная группа, описанная в подпункте (b)(ii) настоящего раздела, должна создать **Исполнительный комитет по талантам в области ИИ национальной безопасности (Комитет по талантам),** состоящий из старших должностных лиц ИИ (или назначенных лиц) из всех агентств Координационной группы, которые желают участвовать. Комитет по талантам должен работать над стандартизацией, расстановкой приоритетов и удовлетворением потребностей в талантах в области ИИ и разработать обновленный набор

общеправительственных процедур для привлечения, найма, развития и удержания талантов в области ИИ и поддержки ИИ для целей национальной безопасности.

Комитет по талантам должен назначить представителя для работы в качестве члена Целевой группы по талантам в области ИИ и технологий, изложенной в Указе президента 14110, помогая выявлять пересекающиеся потребности и решать общие проблемы при найме.

(iv) В течение 365 дней с даты настоящего меморандума и ежегодно в течение как минимум следующих 5 лет Координационная группа, описанная в подпункте (b)(ii) настоящего раздела, должна представить APNSA совместный отчет о консолидации и совместимости усилий и систем ИИ в целях национальной безопасности.

Раздел 7. Определения.

(a) В настоящем меморандуме используются определения, изложенные в разделе 3 Указа президента 14110. Кроме того, для целей настоящего меморандума:

(i) **Термин «безопасность ИИ»** означает механизмы, с помощью которых отдельные лица и организации минимизируют и смягчают потенциальный вред отдельным лицам и обществу, который может возникнуть в результате злонамеренного использования, неправильного применения, сбоев, аварий и непреднамеренного поведения моделей ИИ; систем, которые их интегрируют; и способов их использования.

(ii) **Термин «безопасность ИИ»** означает набор методов защиты систем ИИ, включая данные обучения, модели, способности и жизненные циклы, от кибератак и физических атак, краж и повреждений.

(iii) **Термин «охваченные агентства»** означает агентства в разведывательном сообществе, а также все агентства, как определено в 44 USC 3502(1), когда они используют ИИ в качестве компонента системы национальной безопасности, за исключением Исполнительного управления президента.

(iv) **Термин «критические технические артефакты»** (CTA) означает информацию, обычно относящуюся к одной модели или группе связанных моделей, которая, если бы ею

обладал кто-то другой, а не разработчик модели, существенно снизила бы затраты на воссоздание, достижение или использование возможностей модели. В рамках технической парадигмы, доминирующей в отрасли ИИ сегодня, веса моделей обученной системы ИИ составляют СТА, как и, в некоторых случаях, связанные с ними данные обучения и код. Будущие парадигмы могут полагаться на другие СТА.

(v) **Термин «пограничная модель ИИ»** означает универсальную систему ИИ, близкую к передовым показателям производительности, измеряемой общепринятыми общедоступными эталонными тестами или аналогичными оценками рассуждений, науки и общих возможностей.

(vi) **Термин «Разведывательное сообщество» (РС**) имеет значение, предусмотренное в 50 USC 3003.

(vii) **Термин «модель с открытыми весами»** означает модель, веса которой широко доступны, как правило, посредством публичного выпуска.

(viii) **Термин «Правительство Соединенных Штатов**» означает все агентства, как определено в 44 USC 3502(1).

Раздел 8. Общие положения.

(а) Ничто в настоящем меморандуме не должно толковаться как наносящее ущерб или иным образом влияющее на:

(i) полномочия, предоставленные законом исполнительному департаменту или агентству или их главе; или

(ii) функции директора Управления по управлению и бюджету, связанные с бюджетными, административными или законодательными предложениями.

(б) Настоящий меморандум будет реализован в соответствии с действующим законодательством и при условии наличия ассигнований.

(c) Настоящий меморандум не предназначен для создания и не создает никаких прав или выгод, материальных или процессуальных, подлежащих принудительному исполнению по закону или по праву справедливости любой стороной в отношении Соединенных Штатов, их департаментов, агентств или организаций, их должностных лиц, сотрудников или агентов или любого другого лица.

ДЖОЗЕФ Р. БАЙДЕН-МЛАДШИЙ.

Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence

Источник:
https://www.whitehouse.gov/briefing-room/presidential-actions/2024/10/24/memorandum-on-advancing-the-united-states-leadership-in-artificial-intelligence-harnessing-artificial-intelligence-to-fulfill-national-security-objectives-and-fostering-the-safety-security/

г. Астана Насенкова Людмила ТОО «LINCOMPANY»

www.lincompany.kz