

DOI 10.35775/PSI.2025.119.7.035

УДК 32.327

И.В. СУРМА

кандидат экономических наук,
начальник отдела НАМИБ, доцент кафедры
международной и национальной безопасности
Дипломатической академии МИД РФ,
профессор Академии Военных Наук,
Россия, г. Москва

СТРАТЕГИЯ НАТО В ОБЛАСТИ НАУКИ И ТЕХНОЛОГИЙ: МЕХАНИЗМЫ РЕАЛИЗАЦИИ

В статье рассмотрена эволюция стратегических инициатив НАТО, начиная от военной доминанты и адаптации к научно-технологическому доминированию. Рассмотрена новая Стратегия НАТО в области науки и технологий, принятая в 2025 году, которая предполагает активные инвестиции в критически важные и прорывные технологии, такие как искусственный интеллект, квантовые технологии, автономные системы и кибербезопасность. Подчеркнуто, что в среднесрочной перспективе это приведет к появлению принципиально новых и модернизированных образцов систем вооружения и военной техники, что повысит технологическое превосходство НАТО. Автор обращает внимание на тот факт, что внедрение новых технологий будет сопровождаться усилением защиты научных разработок и оптимизацией процессов от исследований до практического применения на поле боя. Показано, что в совокупности с другими документами стратегического планирования Североатлантического альянса новая Стратегия НАТО в области науки и технологий формирует комплексный подход к обеспечению технологического превосходства, а в сочетании с программами перевооружения означает стремление альянса создать качественно новые военные возможности, что потребует от России существенного наращивания своего научно-технического потенциала и модернизации оборонной промышленности страны.

Ключевые слова: Стратегическая концепция НАТО, Task Force Lima, Саммит НАТО, искусственный интеллект, кибербезопасность, Стратегия ИИ НАТО, глубокие технологии, проект DIANA.

Принятие в июне 2022 года на саммите в Мадриде восьмой Стратегической концепции НАТО (NATO 2022 Strategic Concept) [4], ранее подготовленной в штаб-квартире альянса в Брюсселе и предназначенной в качестве ответа на серьезные геополитические и геоэкономические трансформации, по существу, стало разделительной вехой для Североатлантического альянса. Новая концепция пришла на смену седьмого аналогичного документа, получившего наименование «Активное участие, современная оборона» («Active Engagement, Modern Defence») [2] и принятого на 22-м саммите альянса в Лиссабоне в 2010 г. Концепция 2010 г., была единодушно одобрена в португальской столице

в присутствии руководителей двадцати стран, не входящих в НАТО, и президента Российской Федерации Д.А. Медведева. Такой подход вполне соответствовал декларируемому НАТО в тот период вектору на поддержание международной стабильности и развитие контактов с максимальным числом заинтересованных государств.

Новая Стратегическая концепция [4] определила главные приоритеты функционирования Североатлантического альянса до 2030, ключевая идея которых состоит в том, что Россия объявлена главной угрозой безопасности НАТО в отличие от предыдущей концепции 2010-го года, где она рассматривалась как партнер. В рамках противостояния Российской Федерации, участники форума договорились о существенном расширении военного присутствия стран на восточном направлении и в первую очередь предполагается разместить войска в Прибалтике, Польше и Румынии. Численность сил НАТО высокой готовности увеличится с 40 000 человек до более чем 300 000 человек. Включение Швеции и Финляндии в блок НАТО создает новые угрозы для России, на которые Россия будет вынуждена отвечать.

Кроме того, в Стратегической концепции НАТО, принятой на саммите в Мадриде, Китай официально провозглашается державой, которая бросает вызов интересам, безопасности и ценностям альянса и стремится подорвать международный порядок, основанный на правилах [4]. Страны НАТО выступили против «углубления стратегического партнерства» между Китаем и Россией. Отметим, что в Стратегической концепции НАТО серьезное внимание уделено не только Европе, но и Индо-Тихоокеанскому региону и Северной Африке. А также альянс утвердил пакет помощи Украине, чем продемонстрировал свое намерение серьезно и надолго продолжить конфронтацию с Россией, подпитывая Украину оружием. Все это усиливает вероятность военного столкновения между НАТО и Россией.

Таким образом, принятие на саммите в Мадриде новой Стратегической концепции НАТО, по существу, разделило историческую траекторию Североатлантического альянса на «до» и «после». Более того, вооруженный конфликт на Украине сегодня превратился в первостепенную проблему всей международной деятельности альянса, что не только оказывает влияние на содержание военных программ, но и определяет долгосрочную политику НАТО в Европе и за ее пределами.

Этот факт подтвердил и Юбилейный саммит НАТО, прошедший 9-11 июля 2024 года в Вашингтоне, где была принята декларация, которая явилась, по своей сути, концепцией подготовки войны с Россией и ее союзниками (Китаем, Белоруссией, КНДР, Ираном). Причем в подготовке к этой войне НАТО делает упор на интеграцию новых технологий и инноваций. Поэтому в рамках саммита была представлена обновленная стратегия по развитию технологий искусственного интеллекта (ИИ), нацеленная на укрепление оборонного потенциала НАТО. Пересмотренная стратегия НАТО по ИИ [7] направлена на интеграцию технологий искусственного интеллекта с военными операциями и на устранение

растущей опасности дезинформации и других проблем безопасности. Стратегия представляет собой перечень мер, которые могут помочь минимизировать риски, связанные с использованием искусственного интеллекта в вооруженных силах, гарантируя его ответственное и этическое использование.

Как конкретно НАТО будет использовать генеративный искусственный интеллект (GenAI), остается до конца неясным, но в США, которые значительно опередили Европу в этом плане, есть множество прецедентов. Министерство обороны США, например, стало прикладывать свои усилия на высшем уровне по управлению GenAI, создав новую целевую группу **Task Force Lima**, чтобы лучше понять, как инструменты генеративного искусственного интеллекта (ИИ), такие как большие языковые модели, смогут поддержать его инновационные усилия. Оперативную группу **Task Force Lima** возглавило Главное управление цифровых технологий и искусственного интеллекта **Chief Digital and Artificial Intelligence Office** (CDAO) Пентагона. Эта группа должна оценивать, синхронизировать и использовать генеративные возможности искусственного интеллекта в Министерстве обороны, гарантируя, что министерство останется в авангарде передовых технологий, одновременно защищая национальную безопасность. CDAO работает вместе с офисами заместителей министра обороны США по политике, исследованиям и разработкам, закупкам и поддержке, разведке и безопасности, а также с главным информационным управлением Министерства обороны. Все перечисленные структуры имеют конкретные роли в рамках деятельности оперативной группы **Task Force Lima**.

Разведывательное сообщество США начало применять защищенный чат-бот Microsoft в мае 2024 года, BBC США развернули свой инструмент NIGRGPT в июне 2024 года, а Сухопутные войска США инициировали собственный защищенный проект GenAI в июле 2024 года. В ближайшей перспективе оборонные и разведывательные агентства США сосредоточатся на использовании больших языковых моделей для обработки огромных объемов текста – контрактов, запросов предложений, логистических данных и отчетов военной разведки – с целью составления сводки и, в самых амбициозных случаях, разработки предложений по возможным сценариям операций и планирования.

Другим важным направлением усилий Пентагона в области ИИ в целом, а не только в GenAI, было тщательное тестирование этих технологий для того, чтобы гарантировать правильность работы алгоритмов. Реальное тестирование является достаточно сложным для оборудования, но оно осуществляется еще сложнее с алгоритмами машинного обучения, которые изменяют себя по мере получения новых данных, часто способами, непрозрачными даже для их изначальных разработчиков-программистов. Новая стратегия НАТО по развитию ИИ подхватывает эту идею и расширяет краткие предложения версии 2021 года [5] о тестировании до чего-то гораздо более подробного и директивного. Официальный список направлений в редакции 2024 года призывает НАТО создать ключевые элементы ландшафта тестирования, оценки, верификации

и валидации ИИ в масштабах всего Североатлантического альянса. Для этого используется вся сеть испытательных центров проекта DIANA [3].

Еще одним приоритетом обновленной стратегии по развитию ИИ является улучшение оперативной совместимости между системами ИИ государств-членов НАТО, целью которой является то, чтобы различные технологии могли легко работать вместе в ходе различных военных операций, тем самым повышая общий оборонный потенциал Североатлантического альянса. Обновленная стратегия также затрагивает различные проблемы этики и безопасности, связанные с использованием ИИ в военном контексте. В стратегии определяется порядок действий по противодействию или минимизации таких рисков, как предвзятость, отсутствие прозрачности и возможное злоупотребление технологиями и системами ИИ.

Существует три проблемы связанные с системами ИИ и принятием решений, которые постоянно остаются в центре внимания официальных лиц НАТО. Первая проблема – это вопрос функциональной совместимости систем. Несмотря на то, что в стратегии НАТО в области ИИ признается важность оперативной совместимости, или способности некоторых аспектов системы успешно и эффективно взаимодействовать друг с другом, это остается актуальной проблемой. Если ИИ будет использоваться для поддержки процесса принятия решений в НАТО, то обеспечение успешного доступа к соответствующим данным и обмена ими в нужное время и в нужном месте будет иметь ключевое значение. Но несмотря на то, что интеграция ИИ может улучшить ситуационную осведомленность, обмен данными между системами стран-членов будет непросто.

Вторая проблема – это вопрос о предположении наличия прямой связи между передовыми информационными технологиями и победой в войне. Исследования показали, что системы принятия решений с поддержкой ИИ, если их применять бессистемно, могут легко привести к путанице в условиях военного конфликта и можно пока лишь констатировать факт того, что технологии ИИ как инструмент могут быть полезны. Поэтому в документе отмечается, что НАТО должна бороться с распространенным предположением о том, что ИИ обязательно вносит ясность и точность в войну.

Третья проблема – это вопрос установления стандартов ответственного использования технологий ИИ в военной сфере. Несмотря на то, что в стратегии НАТО по развитию ИИ от 2021 года [7] были изложены основные шесть принципов – законность, ответственность и подотчетность, объяснимость и отслеживаемость, надежность, управляемость и смягчение предвзятости, но каждый из этих принципов потребует от НАТО предоставления уточненных и подробных указаний для стран-членов блока. Кроме того, задача осложняется различными уровнями этических оценок и оценок угроз, а также различным инфраструктурным потенциалом стран альянса. Процесс разработки этических стандартов осложняется еще и тем, что у Североатлантического блока нет механизма обеспечения соблюдения стандартов ответственного использования технологий ИИ. Это только основной спектр проблем, с которыми НАТО столкнулась на пути

к интеграции систем ИИ. Для решения некоторых из указанных проблем, в обновленной стратегии по развитию ИИ определены необходимые практические шаги:

1. Так как координация с самого начала является ключом к предотвращению расхождений в национальных подходах к системной архитектуре и интеграции, а также к решению вопроса о том, как данные должны распределяться между странами-членами, то Комитеты НАТО, такие как Комитет по цифровой политике, должны продолжать свои координационные усилия по обеспечению оперативной совместимости, учитывать уроки, извлеченные из экспериментов и военных игр стран-членов НАТО, и будут продолжать работу по установлению ИИ и цифровых стандартов во всем Североатлантическом альянсе. Не менее важна необходимость создания и курирования целевых и хорошо адаптированных наборов данных для поддержки принятия решений, сценариев использования и оперативного планирования. Такие инициативы могли бы координироваться Советом НАТО по обзору данных и ИИ, которому в настоящее время поручено осуществлять надзор за ответственным внедрением ИИ в рамках всего блока НАТО, а также служить форумом для дискуссий между промышленностью, правительством и научными кругами, исходя из того, что до сих пор не существует «основного» набора сравнительных данных, в котором можно было бы измерить обобщенную производительность ИИ.

2. НАТО должна признать, что, хотя технологии и системы ИИ могут являться важными компонентами, они не являются универсальным решением политических и военных проблем. Эффективное сотрудничество между ИИ и лицами, принимающими решения, потребует тесной интеграции между разработчиками и военными экспертами, начиная с первоначального этапа разработки системы. Более того, это потребует от лиц, принимающих решения, хорошо разбираться в возможных режимах отказа моделей ИИ и быть готовыми использовать собственное экспертное суждение в таких ситуациях. Хотя ИИ может быть инструментом для осмысления мира, он также может привести путаницу и неопределенность в организацию. Таким образом, для того, чтобы добиться результата в выгодном для НАТО направлении, потребуется накопление устойчивых знаний о том, как системы с поддержкой ИИ и люди взаимодействуют на стыке технической и социально-гуманитарной сфер.

3. По мере того, как НАТО будет разрабатывать нормы не только для Североатлантического альянса, но и в глобальном масштабе, необходимо будет быть более прозрачной в отношении характера шести принципов ответственного использования ИИ. В то время как страны-члены НАТО должны открыто общаться, чтобы достичь общего понимания этих принципов, Североатлантический альянс должен обеспечить, чтобы эти принципы не ставили под угрозу военную компетентность государств-членов. Кроме того, эта задача потребует более продуктивного взаимодействия между НАТО и ЕС. До сих пор такое взаимодействие было ограниченным. Несмотря на то, что недавний Закон ЕС об искусственном интеллекте позволяет избежать применения

ИИ в военных целях, двойной характер этих систем, скорее всего, поставит их под действие закона, поэтому при установлении стандартов для этих систем должна быть четко очерчена правовая база.

В документе подчеркивается, что более быстрое и качественное принятие решений не является предопределенным результатом интеграции систем ИИ в проведение операций НАТО. Отмечается, что Североатлантический альянс должен сосредоточиться на вопросах координации между странами-членами, вопросах качества данных и обучения моделей, а также на процессах установления стандартов. При этом считается, что НАТО может выявить эффективные способы использования технологий ИИ, которые смогут помочь в принятии решений.

Таким образом, сегодня инновации и технологии ИИ используются почти во всех военных приложениях. Так в июле 2025 года Министерство обороны США (U.S. Department of Defense, DoD) объявило о заключении контрактов с четырьмя ведущими разработчиками генеративного искусственного интеллекта (generative AI): Google DeepMind – с моделью Gemini; xAI Илона Маска – с моделью Grok; Anthropic – с моделью Claude Opus и OpenAI – с моделью ChatGPT (на базе GPT-4o).

Планируется, что каждая компания получит до 200 миллионов долларов в рамках многолетнего соглашения. Финансирование идет через DIU (Defense Innovation Unit) – подразделение Пентагона, занимающееся интеграцией коммерческих технологий в армию. Суммарный объем на первом этапе может превышать 800 миллионов долларов.

Программа направлена на расширенное использование ИИ в ключевых военных направлениях, таких как: Intelligence Analysis – анализ разведданных (спутниковые снимки, сигналы, видео); Campaign Planning – моделирование операций и оценка рисков; Logistics – оптимизация цепочек поставок, маршрутизация и прогнозирование; Data Collection и File Search – сбор данных из разных каналов и интеллектуальный поиск в архивах.

Каждая модель будет адаптирована под задачи Пентагона с соблюдением следующих требований: Air-gapped systems – офлайн-защищенных сетей; Adversarial robustness – устойчивости к атакам (например, отравление данных); Explainable AI – способности объяснять свои выводы; LOAC compliance – соответствия Праву вооруженных конфликтов, а также требований DoD Directive 3000.09 по автономным и полуавтономным системам.

Например, Claude Gov – специализированная версия ИИ Claude для государственных структур США, уже используется в Lawrence Livermore National Laboratory – исследовательском центре по ядерным технологиям.

Эти контракты стали ответом на усиление конкурентной борьбы за военный ИИ между США, Китаем, Россией и Израилем. Инициатива позволяет преодолеть, так называемую «долину смерти» (Valley of Death) – пропасть между техническими разработками и их практическим внедрением.

В рамках программы будут реализованы следующие направления: Secure data centers – защищенные серверные центры; AI infrastructure – кластеры GPU и каналы связи; Training programs – обучение военных персонала работе с ИИ.

Таким образом, суммарные инвестиции в размере 800 миллионов долларов будут направлены не в чат-ботов, а в цифровые штабные решения – киберофицеров для разведки, планирования и логистики. Это ключевой сдвиг в военной парадигме, когда нейросети заменяют стратегический анализ, и страны, которые не успевают за развитием систем ИИ, окажутся в весьма уязвимом положении.

Поэтому увеличение финансирования разработок со стороны военных исследовательских агентств и стран-членов НАТО для создания новых и передовых способов использования ИИ приведет к расширению его применения в военных целях. Подтверждением этого процесса является Декларация Вашингтонского саммита НАТО [8], в которой отмечается ускорение трансформации Североатлантического альянса, чтобы противостоять текущим и будущим угрозам и сохранить технологическое превосходство НАТО, в том числе за счет более быстрого внедрения новых технологий и цифровой трансформации. С этой целью НАТО планирует быструю реализацию пересмотренной Стратегии в области искусственного интеллекта и новых Стратегий в области квантовых технологий и биотехнологий, для чего будет использован успех Североатлантического инновационного центра оборонных инноваций (DIANA) и Инновационного фонда НАТО (NIF).

5 июня 2025 года министры обороны стран НАТО встретились в Брюсселе в преддверии саммита в Гааге. На встрече были согласованы целевые показатели нового плана инвестиций в оборону, для их утверждения на саммите альянса в Гааге. В частности, в новом плане союзников по НАТО было предложено к 2035 году вкладывать в оборону ежегодно 5% ВВП, в том числе 3,5% в ключевые силы и средства и 1,5% ВВП на расходы, связанные с обороной и безопасностью, в частности в инфраструктуру и стрессоустойчивость. Также государства-члены союза на встрече в Брюсселе обязались предоставить в 2025 году Украине дополнительную помощь в области безопасности в размере свыше 20 миллиардов евро. Кроме того, на заседании Группы ядерного планирования НАТО в ходе министерской встречи генеральный секретарь альянса Марк Рютте заявил о том, что ядерное сдерживание остается краеугольным камнем безопасности Североатлантического союза, и необходимо обеспечить силу и эффективность ядерного потенциала НАТО ради сохранения мира, недопущения принуждения и сдерживания агрессии.

Важно, что 5 июня 2025 года также была утверждена новая Стратегия НАТО в области науки и технологий, отражающая кардинальное изменение подхода Североатлантического альянса к технологическому превосходству в условиях нарастающей геополитической напряженности и быстрого развития инновационных технологий. Стратегия НАТО в области науки и технологий, определяет единую политику в сфере научных исследований, технологических разработок и инноваций в интересах обеспечения коллективной безопасности альянса [6].

Стратегия определяет три ключевые цели: во-первых, предвидение и инвестирование в перспективные технологии, для того, чтобы опережать стратегических конкурентов; во-вторых, защита научно-технической деятельности от угроз (шпионажа и неправомерного использования) и, в-третьих, координация усилий между гражданскими и военными исследователями для ускоренного внедрения инноваций в военную сферу. В качестве приоритетных областей научно-исследовательской деятельности в документе выделяются: искусственный интеллект, кибербезопасность, квантовые технологии, биотехнологии, автономные системы и новые материалы. Также значимое место в новом документе уделено вопросам этики, управления данными, защиты интеллектуальной собственности и обеспечения доверия к новым технологиям.

Механизм реализации Стратегии НАТО в области науки и технологий основан на развитии партнерских программ с международными организациями, научными центрами и промышленностью стран-членов альянса, активизации деятельности Научно-технологической организации НАТО (NATO Science and Technology Organization – STO) и усилении координации между странами-членами альянса, а также особое значение придается формированию единого научного пространства, которое будет обеспечивать обмен знаниями, совместное проведение научно-прикладных исследований и внедрение инноваций. Важным инструментом реализации также является развитие образовательных и научно-исследовательских проектов. Это актуальные вопросы подготовки кадров, с соответствующими компетенциями в области передовых технологий и способных эффективно отвечать на новые вызовы и угрозы безопасности. Подчеркивается необходимость поддержания высокого уровня научной экспертизы и постоянного обновления знаний в условиях быстро изменяющейся технологической среды. В документе придается приоритетное значение сотрудничеству с международными организациями, что будет способствовать обмену знаниями и координации усилий в сфере научно-технологического развития. Кроме того, неотъемлемым элементом инновационной политики, обеспечивающим доступ к передовым разработкам, ускоряющим внедрение новых технологий и способствующим формированию устойчивой экосистемы безопасности является взаимодействие с гражданским сектором.

Также в документе подчеркивается важность соблюдения международных стандартов, этических норм и принципов транспарентности при реализации научно-технологических инициатив. Особое внимание уделяется вопросам обеспечения кибербезопасности и предотвращения злоупотреблений в сфере новых технологий.

Следует отметить, что одним из важных нововведений Стратегии НАТО в области науки и технологий является проактивное управление технологическими рисками, предусматривающее создание систем раннего предупреждения, мониторинга угроз и быстрого реагирования на инциденты, связанные с использованием новых технологий в военных и гражданских целях. Стратегия предполагает развитие механизмов оценки и валидации новых технологий, а также

формирование нормативно-правовой базы, регулирующей их применение в интересах коллективной безопасности. Поэтому вопросы киберустойчивости, защиты от информационных атак и предотвращения утечек чувствительных данных становятся одними из приоритетных [1. С. 78-85].

Сегодня внедрение инноваций является центральным элементом трансформации системы коллективной обороны Североатлантического альянса. В Стратегии НАТО в области науки и технологий упор делается на необходимость интеграции новых технологий на всех уровнях – от стратегического планирования до оперативного и тактического управления. Особое значение придается развитию платформ для обмена знаниями, созданию совместных исследовательских проектов и стимулированию предпринимательской активности в сфере оборонных технологий.

Таким образом, Стратегии НАТО в области науки и технологий закрепляет переход от реактивной к проактивной модели управления инновациями, предусматривающей постоянный анализ новых технологических направлений, выявление наиболее перспективных и оперативное внедрение результатов научных исследований в практику обеспечения обороны и безопасности. Важным результатом реализации такой стратегии станет повышение уровня готовности НАТО к реагированию на гибридные угрозы, обеспечение технологического лидерства и формирование устойчивой системы управления рисками в условиях нарастающей геополитической нестабильности и неопределенности.

В совокупности с другими документами стратегического планирования Североатлантического альянса новая Стратегия НАТО в области науки и технологий формирует комплексный подход к обеспечению технологического превосходства, а в сочетании с программами перевооружения означает стремление альянса создать качественно новые военные возможности, что потребует от России существенного наращивания своего научно-технического потенциала и модернизации оборонной промышленности страны.

В заключение отметим, что на официальной сессии глав государств и правительств стран НАТО 25 июня 2025 года лидеры стран-членов альянса приняли декларацию саммита, которая одобрила повышение расходов на оборону до 5% от ВВП.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. Гриняев С.Н. Эволюция долгосрочных ориентиров НАТО в XXI веке: анализ новой стратегии в области науки и технологий // Аналитические записки Института Европы РАН. (Выпуск II) № 20. 2025 (№ 388).
2. Active Engagement, Modern Defence // https://www.nato.int/cps/en/natohq/official_texts_68580.htm.
3. Defence Innovation Accelerator for the North Atlantic (DIANA) // https://www.nato.int/cps/en/natohq/topics_216199.htm.

4. NATO 2022 Strategic Concept // https://www.nato.int/cps/en/natohq/topics_210907.htm.
5. NATO: Summary of the NATO Artificial Intelligence Strategy, 22.10.2021 // https://www.nato.int/cps/en/natohq/official_texts_187617.htm.
6. NATO releases new Science & Technology Strategy. NATO. 11.06.2025 // https://www.nato.int/cps/en/natohq/news_236107.htm.
7. Summary of NATO's revised Artificial Intelligence (AI) strategy. 10.07.2024 // https://www.nato.int/cps/en/natohq/official_texts_227237.htm.
8. Washington Summit Declaration issued by the NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Washington, D.C. 10 July 2024 // https://www.nato.int/cps/en/natohq/topics_216199.htm.

I.V. SURMA

Candidate of Economic Sciences,

Head of the Department of the National Association for International Information Security, Associate Professor of the Department of International and National Security of the Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation; professor of the Academy of Military Sciences, Moscow, Russia

NATO'S SCIENCE AND TECHNOLOGY STRATEGY: IMPLEMENTATION MECHANISMS

The article examines the evolution of NATO's strategic initiatives, starting from military dominance and adaptation to scientific and technological dominance. The new NATO Science and Technology Strategy, adopted in 2025, is considered, which involves active investments in mission-critical and breakthrough technologies such as artificial intelligence, quantum technologies, autonomous systems and cybersecurity. It was emphasized that in the medium term, this will lead to the emergence of fundamentally new and modernized models of weapons systems and military equipment, which will increase the technological superiority of NATO.

The author draws attention to the fact that the introduction of new technologies will be accompanied by increased protection of scientific developments and optimization of processes from research to practical application on the battlefield. It is shown that, together with other strategic planning documents of the North Atlantic Alliance, the new NATO Strategy in the field of science and technology forms an integrated approach to ensuring technological superiority, and in combination with rearmament programs means the alliance's desire to create qualitatively new military capabilities, which will require Russia to significantly increase its scientific and technical potential and modernize the country's defense industry.

Key words: NATO Strategic Concept, Task Force Lima, NATO Summit, artificial intelligence, cybersecurity, NATO AI Strategy, deep technology, Project DIANA.