

DOI 10.35775/PSI.2026.127.3.025

УДК 32.327

И.В. СУРМА

кандидат экономических наук,
доцент кафедры прикладного анализа международных проблем
Дипломатической академии МГИМО МИД РФ,
Вице-президент НИИГлоБ,
Россия, г. Москва

НАТО И ЕС: СТРАТЕГИЯ РАЗВИТИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И КВАНТОВЫХ ТЕХНОЛОГИЙ

Эволюция стратегий стран ЕС и НАТО в области развития искусственного интеллекта (ИИ) и квантовых технологий отражает стремление альянса укрепить технологическое превосходство, повысить обороноспособность и противостоять современным угрозам. За последние годы НАТО существенно расширило подходы к интеграции этих технологий, акцентируя внимание на ответственности, совместности, сотрудничестве и защите от потенциальных рисков. В статье рассматривается эволюция военно-технической стратегии НАТО в области искусственного интеллекта (ИИ) и квантовых технологий в период 2018-2025 гг. – от запуска «Инициативы по ИИ» (2018) до создания первого в истории Альянса Квантового центра и публикации обновленной «Стратегии квантово-устойчивой безопасности» (2025). Рассматриваются этапы трансформации и анализируется стратегия ЕС в области квантовых технологий. Делается вывод о переходе ЕС и НАТО от оборонительной цифровой модернизации к наступательной технологической конкуренции, синхронизирующей развитие ИИ и квантовых технологий для обеспечения доминирования в сферах связи, криптографии и управления войсками.

Ключевые слова: НАТО, искусственный интеллект, CWIX-2025, постквантовая криптография, DIANA, квантовое распределение ключей, Трансатлантическое квантовое сообщество, ЕС.

Рассматривая эволюцию подходов Североатлантического альянса (НАТО) к разработке и внедрению технологий искусственного интеллекта (ИИ) и квантовых вычислений в военной сфере проанализируем ключевые этапы трансформации стратегии НАТО: от разрозненных национальных инициатив (середина 2010-х гг.) к формированию единой союзнической политики (2020-2024 гг.). Особое внимание следует уделить программным документам НАТО, включая «Стратегию по ИИ» (2021 г.) [8], созданию Центра квантовых технологий (2023 г.) [1] и механизмам Фонда инноваций (DIANA). Безусловно, необходимо не исключать и проблемы совместимости систем, этические ограничения применения

автономного оружия, а также риски технологического отставания от основных противников Североатлантического альянса, и, прежде всего, КНР и России.

Можно выделить основные хронологические этапы:

2018-2020 гг. – децентрализованные национальные программы США, Великобритании и Франции, отсутствие единых стандартов ИИ для систем C4ISR;

2021 г. – принятие первой «Стратегии НАТО по ИИ» [8], запрет на использование ИИ в системах ядерного управления, создание Совета по ИИ;

2022-2023 гг. – ответ на опыт войны в Украине: ускоренное внедрение ИИ для анализа данных с БПЛА и спутников; создание Фонда инноваций DIANA (1 млрд евро на квантовые и ИИ-проекты) [6];

2024 г. – запуск Центра квантовых технологий НАТО, приоритет – постквантовая криптография (PQC) для защиты сетей связи от атак с использованием квантовых компьютеров;

2025 г. – интеграция ИИ и квантового распределения ключей (QKD): новые протоколы для управления автономными системами поля боя.

Эволюция стратегии в области ИИ. Первая стратегия НАТО в области ИИ была утверждена в октябре 2021 года [8]. Она устанавливала нормативы по ответственному использованию ИИ в соответствии с международным правом. В документе были представлены «Принципы ответственного использования ИИ в обороне», включающие законность, ответственность, объяснимость, надежность и смягчение предвзятости.

Обновленная стратегия по ИИ была опубликована 10 июля 2024 года. Она учитывает технологические прорывы последних лет и ставит ряд новых задач:

– **Интеграция ответственного ИИ в деятельность НАТО.** Альянс стремится стать примером ответственного использования ИИ и влиять на формирование международных норм в этой сфере.

– **Ускорение внедрения ИИ в разработку и внедрение возможностей.** Планируется усилить интеграцию ИИ в планирование обороны, а также повысить оперативную совместимость систем ИИ стран-членов для эффективного взаимодействия в военных операциях.

– **Защита технологий ИИ и управление рисками.** НАТО намерено привлекать квалифицированных тестировщиков из частного сектора, госорганов и научных учреждений для аккредитации и сертификации систем ИИ. Будут приняты общие для альянса методы тестирования, оценки, верификации и валидации ИИ (TEV&V), применяемые в проекте DIANA (Defence Innovation Accelerator for the North Atlantic) [6].

– **Противодействие угрозам, связанным с использованием ИИ противником.** Стратегия учитывает риски, связанные с применением ИИ для дезинформации, деморализации обществ и военных сил, а также для проведения информационных операций.

Особое внимание в обновленной стратегии уделяется конвергенции ИИ с другими прорывными технологиями, включая квантовые.

Развитие стратегии в области квантовых технологий. Квантовая стратегия НАТО была утверждена министрами иностранных дел стран альянса 28 ноября 2023 года [2], а краткое резюме опубликовано 17 января 2024 года. В ней описываются возможности применения квантовых технологий в сфере обороны и безопасности, например:

- зондирование и визуализация;
- точное позиционирование, навигация и синхронизация;
- оптимизация обнаружения подводных лодок;
- модернизация и обеспечение безопасности передачи данных с помощью квантово-устойчивой криптографии.

Ключевые цели квантовой стратегии:

- стать «квантово готовым» альянсом;
- использовать квантовые технологии для поддержки основных задач НАТО;
- развивать сотрудничество с промышленностью и научными кругами для создания трансатлантической экосистемы квантовых технологий;
- защищаться от злонамеренного использования квантовых технологий.

В стратегии подчеркивается, что конвергенция квантовых технологий с другими электронными технологиями влечет важные последствия для обороны и безопасности, а также потенциальные военные применения. Среди перспективных направлений – квантовые вычисления для криптографии, оптимизации логистики и разведки, квантовая криптография для защиты данных, квантовые сенсоры для сверхточной навигации и обнаружения объектов.

Для реализации стратегии было создано **Трансатлантическое квантовое сообщество** [7]. Оно объединяет экспертов из национальных правительств, промышленности, академических кругов, финансирующих органов и научно-исследовательских институтов. Сообщество призвано способствовать развитию инноваций и защите технологического преимущества НАТО.

Из представленной хронологии видно, что эволюция стратегии НАТО в указанных сферах характеризуется переходом от изолированного развития ИИ и квантовых технологий к их конвергентному применению. Если ИИ отвечает за скорость обработки данных и автономность решений, то квантовые технологии обеспечивают не взламываемую связь (через QKD) и возможность дешифровки коммуникаций противника (квантовый криптоанализ). В период 2018–2025 гг. Альянс прошел путь от признания квантовой угрозы для существующих алгоритмов шифрования (RSA, ECC) до создания операционных механизмов постквантовой безопасности. Сегодня квантовая угроза для традиционной криптографии подталкивает НАТО переводить системы управления ИИ на постквантовые стандарты шифрования, чтобы избежать, так называемого, «сценария Q-Day» (дня, когда квантовый компьютер ломает всю текущую защиту). Косвенно можно сделать вывод, что в ближайшие два года НАТО планирует достичь технологической синхронизации, при которой каждый ИИ-агент на поле боя будет

сертифицирован квантово-устойчивым ключом, а разведывательные данные – обрабатываться гибридными (ИИ + квантовые сенсоры) системами.

Так как внедрение ИИ в управление войсками, разведку и автономные системы делает их уязвимыми для атак с использованием квантовых компьютеров («квантовый Q-Day»), НАТО разворачивает двухуровневую систему квантовой криптографии:

1. Квантовое распределение ключей (QKD) – для защиты линий связи между командными центрами и ИИ-платформами (БПЛА, роботизированные системы) от перехвата.

2. Постквантовая криптография (PQC) – для перевода всех ИИ-алгоритмов, работающих в полевых условиях, на квантово-устойчивые стандарты шифрования (алгоритмы на основе решеток).

Проанализировав ключевые решения НАТО, такие как: создание Центра квантовых технологий в Копенгагене (2023) и квантового центра в Лейпциге (2024), интеграция QKD в программу DIANA (2023-2025) [7; 1], а также первые полевые испытания квантово-защищенных каналов для передачи данных между ИИ-анализаторами спутниковой разведки (учение «CWIX-2025» [5]), можно сделать вывод, что эволюция стратегии НАТО в квантовой криптографии перешла от оборонительной (защита существующих ИИ-систем) к **наступательной**. Поэтому в структурах НАТО разрабатываются методы квантового криптоанализа для взлома шифров противника с использованием гибридных ИИ-квантовых алгоритмов. При этом главным вызовом остается стандартизация PQC для всех 32 стран-членов НАТО к 2027 году.

Учения НАТО CWIX 2025. Несмотря на то, что открытые источники не содержат детального описания протоколов именно этого учения, «первые полевые испытания» квантово-защищенных каналов для передачи данных ИИ-анализаторов спутниковой разведки, которые вы запросили, по всей видимости, являются частью комплексной программы НАТО **CWIX 2025** (Coalition Warrior Interoperability Exercise) [5]. Ее ключевой технологический фонд и логику можно описать на основе реальных тестов и инфраструктуры, которая была задействована.

Учения прошли со **2 по 20 июня 2025 года** в польском городе Быдгощ в Joint Force Training Centre (JFTC). В них участвовало почти **3 000 человек** из 42 стран (все 32 члена НАТО и партнеры, включая Украину), было проверено более 570 систем и выполнено свыше 25 000 тестов. Среди них – отработка взаимодействия в космосе (Space Situational Awareness) и интеграции спутниковых данных в единую сеть управления, где использовались ИИ-алгоритмы для обработки информации.

Квантовая защита: от лаборатории к полю. Связка «спутник – ИИ» в НАТО защищается двумя способами. Один из них – квантовое распределение ключей (QKD), позволяющее создавать абсолютно стойкие ключи шифрования. Другой – пост-квантовая криптография (PQC), защищающая данные от атак будущих квантовых компьютеров.

Важнейшим практическим шагом стало успешное создание в июне 2025 года первого трансатлантического квантово-защищенного канала между акселераторами NATO DIANA (в Копенгагене и Галифаксе). Компания Quantropi использовала PQC-слой QiSpace™, а Alea Quantum – квантовые генераторы случайных чисел (QRNG). В результате сеть работала в реальном времени без установки специализированного оборудования на конечных устройствах, что критически важно для полевых условий.

Исходя из открытых данных можно представить потенциальный сценарий проведения учений:

1. Данные со спутника: Низкоорбитальный спутник наблюдения передавал зашифрованные изображения на наземную станцию.

2. Защищенный канал (QKD/PQC): Передача данных защищалась квантовыми ключами, сгенерированными на основе оптоволоконных или спутниковых QKD-решений, как в проектах центра VTT (VTT – Technical Research Centre of Finland). Ключи генерировались и распространялись по протоколам квантовой связи, гарантируя их абсолютную стойкость к перехвату.

3. Анализ ИИ: На серверах командного центра ИИ-анализатор обрабатывал этот зашифрованный поток.

4. Результат: ИИ формировал разведданные, которые передавались обратно конечным пользователям по тому же защищенному каналу.

Такой подход закрывает ключевую проблему: злоумышленник (противник) не может незаметно перехватить ключ шифрования или подменить данные от спутника на этапе передачи.

Эти испытания стали важной демонстрацией готовности НАТО защищать свой «цифровой каркас» от будущих угроз с помощью квантовой криптографии. Это был критический шаг от теоретических концепций к практическим инструментам для поля боя.

Взаимосвязь ИИ и квантовых технологий в стратегии НАТО. В стратегических документах НАТО неоднократно указывается на взаимопроникновение ИИ и квантовых технологий. Их конвергенция открывает новые возможности, например:

- квантовые вычисления ускоряют обучение моделей ИИ;
- ИИ помогает в квантовой коррекции ошибок, повышая надежность систем.

Среди направлений интеграции отметим:

- использование ИИ для анализа данных, получаемых с квантовых сенсоров;
- прогнозирование угроз и управление автономными системами с помощью ИИ и квантовых алгоритмов;
- применение ИИ и квантовой криптографии для киберзащиты.

Можно констатировать, что внешне обе стратегии акцентируют внимание на:

1. Ответственном использовании технологий. Подчеркивается необходимость соблюдения международного права, этических норм и принципов надежности.

2. Координации между странами-членами. Важна совместимость систем, стандартизация и сотрудничество в разработке технологий.

3. Защите от угроз. Учитываются риски, связанные с возможным использованием этих технологий противником.

Среди вызовов, отмеченных в обеих стратегиях – подчеркнута необходимость ускорения разработки технологий, предотвращения «пробелов в возможностях» в условиях конкуренции, а также управления этическими и устойчивыми аспектами инноваций.

Эволюция стратегии Европейского союза (ЕС) в области квантовых технологий. Изменение стратегии ЕС отражает переход от разрозненных инициатив к комплексной программе, направленной на достижение технологического суверенитета, экономической конкурентоспособности и лидерства на глобальном рынке. Этот процесс включал несколько ключевых этапов, связанных с формированием институциональных механизмов, наращиванием инвестиций и адаптацией к новым вызовам.

Начальный этап: формирование основ (2010-е годы). Формально триггером для последовательной разработки единой европейской квантовой системы послужило принятие в 2016 году «Квантового манифеста» (The Quantum Manifesto), который определил общую стратегию для ЕС в области квантовых технологий. Далее в 2018 году был создан Флагман квантовых технологий (Quantum Technologies Flagship) – это инициатива, которая объединила европейские исследовательские институты, промышленность и государственные организации для консолидации передового опыта в четырех ключевых направлениях: квантовые вычисления, квантовое моделирование, квантовая связь и квантовое зондирование и метрология. Программа была рассчитана на 10 лет (2018–2027 гг.) и Еврокомиссия выделила бюджет в 1 млрд евро. Достижением этого периода явились успешные проекты в области квантовой связи, включая соединение квантовых процессоров через промежуточный узел и установление общей связки между несколькими автономными квантовыми процессорами, что стало шагом к созданию квантовой сети.

В последующий период активизировались национальные программы стран-членов ЕС. Например: Германия в 2018 году выделила 650 млн евро на развитие квантовых технологий, позже увеличив финансирование до 2 млрд евро. Одним из достижений стало создание первого национального квантового компьютера [3]. Франция в 2021 году анонсировала пятилетнюю стратегию с бюджетом 1,8 млрд евро, где основное внимание уделялось разработке квантовых компьютеров для применения в фармацевтике, энергетике и транспортной логистике [3]. Также в 2021 году были созданы:

– Европейское совместное предприятие по высокопроизводительным вычислениям (EuroHPC JU) с бюджетом около 7 млрд евро на 2021–2027 годы,

направленное на развитие высокопроизводительных вычислительных систем, включая квантовые компьютеры [4].

– Некоммерческий Европейский консорциум квантовой индустрии (QuIC), призванный способствовать развитию коммерческого сектора квантовых технологий.

Принятие комплексной стратегии (2025 год). В июле 2025 года Еврокомиссия представила Quantum Europe Strategy – стратегию, направленную на превращение Европы в мирового лидера в области квантовых технологий к 2030 году. Документ охватывал несколько следующих взаимосвязанных направлений:

– **исследования и инновации** – объединение усилий по всей Европе для достижения лидерства в квантовой науке и ее промышленной трансформации.

Развитие инфраструктуры – создание масштабируемых, скоординированных инфраструктурных центров для поддержки производства, проектирования и разработки приложений.

– **Укрепление квантовой экосистемы** – инвестиции в быстрорастущие компании, обеспечение безопасности цепочек поставок и индустриализация квантовых технологий.

– **Технологии двойного назначения (безопасность и оборона)** – интеграция безопасных и суверенных квантовых технологий в европейские стратегии в области космоса, безопасности и обороны.

– **Квантовые навыки** – формирование разнообразной рабочей силы через координированное образование, обучение и мобильность талантов.

Среди конкретных инициатив: запуск программы поддержки фундаментальных исследований и разработки прикладных решений в государственном и промышленном секторах (**Quantum Europe Research and Innovation Initiative**); создание «квантовой» проектировочной площадки и шести пилотных линий по выпуску квантовых чипов; запуск предприятия в сфере европейского квантового интернета (**European Quantum Internet**); расширение сети кластеров квантовой компетенции (**Quantum Competence Clusters**).

К 2030 году планируется развернуть полностью работоспособную квантово-безопасную коммуникационную сеть, а к 2035 году – достичь масштаба в 1000 кубитов с поддержкой коррекции ошибок.

Вызовы и перспективы. Среди ключевых вызовов, которые учитывает стратегия выделяются следующие:

– **отставание в коммерциализации** – ЕС до недавнего времени занимал третье место в мире по патентам в области квантовых технологий после США и Китая.

– **Фрагментация усилий** – разрозненность стратегий и дорожных карт между странами-членами ЕС.

– **Дефицит инвестиций** – только 5% глобальных частных инвестиций в квантовые технологии направлялись в ЕС.

– **Кадровый дефицит** – нехватка специалистов в прикладных областях, таких как квантовое ПО и кибербезопасность.

Поэтому для координации реализации стратегии планировалось создать Консультативный совет, в который должны войти ведущие ученые и эксперты, включая лауреатов Нобелевской премии. Также Еврокомиссия анонсировала публикацию закона о квантовых технологиях в 2026 году, который призван помочь в укреплении квантовой системы, улучшить координацию между странами и упростить переход от научных открытий к коммерческим продуктам.

Таким образом, эволюция стратегии ЕС в области квантовых технологий прошла путь от отдельных проектов до комплексной программы, нацеленной на достижение технологического суверенитета, укрепление экономической безопасности и лидерство на глобальном рынке. Однако успех реализации зависит от решения таких проблем, как фрагментация усилий, дефицит инвестиций и кадров. А исходя из того, что в новой стратегии национальной безопасности США перекладывает всю нагрузку в Североатлантическом альянсе на европейские страны, то в совокупности с трансформацией стратегии НАТО в области ИИ и квантовых технологий можно говорить о переходе от оборонительной (защита существующих ИИ-систем) к наступательной стратегии, от общих принципов к конкретным действиям, направленным на укрепление технологического лидерства стран членов ЕС и НАТО в условиях быстроменяющегося геополитического и геоэкономического ландшафта.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. В Копенгагене открылся центр квантовых технологий НАТО // <https://tass.ru/mezhdunarodnaya-panorama/18878527> (дата обращения 20.04.2026).
2. Главы МИД стран НАТО одобрили первую стратегию по квантовым технологиям. 28 ноября 2023 г. // <https://tass.ru/mezhdunarodnaya-panorama/19403711> (дата обращения 20.04.2026).
3. Европейский Союз развивает инвестиции в квантовые технологии: курс на технологическую независимость // <https://components.ru/news/EC-razvivaet-kvantovyye-tehnologii/> (дата обращения: 30.04.2026).
4. Европейский союз на пути к цифровому суверенитету? // <https://ii.org.ru/evropejskij-soyuz-na-puti-k-cifrovomu-suverenitetu-prodolzhenie/> (дата обращения: 30.04.2026).
5. CWIX 2025 (Coalition Warrior Interoperability Exercise). February 4, 2025 // <https://space-coe.org/cwix-2025/> (дата обращения: 20.04.2026).
6. Defence Innovation Accelerator for the North Atlantic (DIANA) // <https://www.nato.int/en/about-us/organization/nato-structure/defence-innovation-accelerator-for-the-north-atlantic-diana> (дата обращения 20.04.2026).
7. NATO Secretary General calls for creation of a transatlantic quantum community, welcomes Denmark's leadership. 29 September 2023 // <https://www.nato.int/en/news-and-events/articles/news/2023/09/29/>

nato-secretary-general-calls-for-creation-of-a-transatlantic-quantum-community-welcomes-denmarks-leadership (дата обращения: 20.04.2026).

8. Summary of NATO's revised Artificial Intelligence (AI) strategy. 10 July 2024 // <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy> (дата обращения 20.04.2026).
9. Summary of NATO's Quantum Technologies Strategy // <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/01/16/summary-of-natos-quantum-technologies-strategy> (дата обращения 20.04.2026).

I.V. SURMA

Candidate of Economic Sciences,
Associate Professor of the Department of Applied Analysis of International Problems
the MGIMO Diplomatic
Academy of the Ministry of Foreign Affairs of the Russian
Federation, Vice President NIIGloB,
Moscow, Russia

NATO AND THE EU: STRATEGY FOR THE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE AND QUANTUM TECHNOLOGIES

The evolution of the strategies of the EU and NATO countries in the field of artificial intelligence (AI) and quantum technologies reflects the alliance's desire to strengthen technological superiority, increase defense capabilities and counter modern threats. In recent years, NATO has significantly expanded its approaches to integrating these technologies, focusing on responsibility, compatibility, cooperation, and protection from potential risks. The article examines the evolution of NATO's military-technical strategy in the field of artificial intelligence (AI) and quantum technologies in the period 2018-2025 – from the launch of the AI Initiative (2018) to the creation of the first-ever Quantum Center Alliance and the publication of the updated Quantum Sustainable Security Strategy (2025). The stages of transformation are considered and the EU strategy in the field of quantum technologies is analyzed. The conclusion is drawn about the transition of the EU and NATO from defensive digital modernization to offensive technological competition, synchronizing the development of AI and quantum technologies to ensure dominance in the fields of communications, cryptography and command and control.

Key words: NATO, artificial intelligence, CWIX-2025, post-quantum cryptography, DIANA, quantum key distribution, Transatlantic Quantum Community, EU.