

ИТОГОВЫЙ ДОКУМЕНТ

МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ

*«Законодательное регулирование противодействия использованию
искусственного интеллекта и новых технологий в террористических целях»*

Санкт-Петербург, Российская Федерация

17 апреля 2025 года



Настоящий документ не содержит официальных выводов и не представляет собой исчерпывающий перечень всех вопросов, поднятых в ходе Конференции. В нем собраны важные моменты, основные выводы и рекомендации для возможного будущего использования. Контртеррористическое управление Организации Объединенных Наций (КТУ ООН) стремится обеспечить точность и актуальность представленной информации, однако не делает никаких заявлений и не дает гарантий, явных или подразумеваемых, в отношении полноты, точности или достоверности текста документа. Представленные в документе мнения и рекомендации служат исключительно в справочных целях и не должны толковаться как окончательные или исчерпывающие.

1. РЕЗЮМЕ

17 апреля 2025 года в Санкт-Петербурге (Российская Федерация) в рамках пятьдесят восьмого пленарного заседания Межпарламентской Ассамблеи государств — участников Содружества Независимых Государств (МПА СНГ) состоялась Международная конференция *«Законодательное регулирование противодействия использованию искусственного интеллекта и новых технологий в террористических целях»*. Конференция была организована Программным офисом [Контртеррористического управления Организации Объединенных Наций \(КТУ ООН\) по парламентскому взаимодействию в сфере предотвращения терроризма и противодействия ему](#) при поддержке [Совета Шуры Государства Катар](#) и в сотрудничестве с [Межпарламентской ассамблеей государств — участников Содружества Независимых Государств \(МПА СНГ\)](#) и [Международным комитетом Красного Креста \(МККК\)](#).

Конференция собрала более 120 участников, представляющих национальные парламенты, региональные и международные парламентские ассамблеи, международные и региональные организации, [технологические] компании частного сектора, научно-академическую сферу и гражданское общество. Среди представленных парламентских ассамблей были [Африканский парламентский союз](#), [Арабский парламент](#), [Азиатская парламентская ассамблея](#), [Межпарламентская ассамблея государств — участников Содружества Независимых Государств \(МПА СНГ\)](#), [Парламентская ассамблея стран Черноморского экономического сотрудничества \(ПАЧЭС\)](#), [Парламентская ассамблея стран Средиземноморья \(ПАС\)](#), [Парламентская ассамблея Организации по безопасности и сотрудничеству в Европе \(ПА ОБСЕ\)](#), [Парламент стран Латинской Америки и Карибского бассейна](#), [Парламентский союз государств — членов Организации исламского сотрудничества](#) и [Парламентская ассамблея тюркских государств \(ТЮРКПА\)](#).

В дискуссиях приняли участие представители [отдела кибербезопасности и новых технологий КТУ ООН](#), [Исполнительного директората Контртеррористического комитета \(ИДКТК\) Совета Безопасности ООН](#), [МККК](#) и региональных организаций в сфере безопасности, включая [Региональную антитеррористическую структуру Шанхайской организации сотрудничества \(РАТС ШОС\)](#), Секретариат ШОС и [Антитеррористический центр Содружества Независимых Государств \(АТЦ СНГ\)](#). С докладами также выступили представители компаний частного сектора и академических учреждений, в том числе Научно-исследовательского центра Федеральной службы безопасности (ФСБ) России, ООО «НОТБОТ» Республики Беларусь, [ассоциации «РУССОФТ»](#), [PIX Robotics](#) и [университета ИТМО](#) (Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики).

Конференция была организована в соответствии с четырьмя тематическими направлениями: i) точки зрения и усилия парламентов; ii) международные организации, стандарты и правовые рамки; iii) сектор безопасности и правоохранительная деятельность; iv) компании частного сектора, научно-исследовательские центры и академические учреждения. Обсуждения были сосредоточены на последствиях использования

искусственного интеллекта и новых технологий как в террористических целях, так и в контртеррористической деятельности. Особое внимание было уделено проблемам надзора и подотчетности, гуманитарным рискам и существующим правовым и этическим проблемам, связанным с этими технологиями.

Участники подчеркнули необходимость применения подходов к регулированию, основанных на соблюдении прав человека, гарантирующих соответствие нормам международного гуманитарного права (МГП) и международного права в области прав человека (МППЧ) и при этом направленных на решение обоснованных проблем в сфере безопасности. Конференция предоставила возможности для ведения диалога о сложностях управления искусственным интеллектом (ИИ), способствовала выявлению передовой практики и заложила основы для разработки модельного законодательства. Она также позволила укрепить межведомственное сотрудничество между КТУ ООН, МПА СНГ, МККК и национальными парламентами и сформулировать руководящие принципы для будущих законодательных инициатив, направленных на обеспечение этического, законного и безопасного использования ИИ в контртеррористической деятельности.

2. СПРАВОЧНАЯ ИНФОРМАЦИЯ

В последние годы искусственный интеллект проявил себя как одна из наиболее трансформирующих сил нашего времени. Его потенциал кардинальным образом изменять науку, государственные услуги и отрасли порождает растущие сомнения в отношении непредвиденных последствий для обществ и правительств стран по всему миру. Помимо экономических и социальных последствий, таких как исчезновение рабочих мест и повышение уязвимости общества, ИИ создает серьезные проблемы в сфере безопасности. Его стремительное развитие и все более доступные возможности вызывают тревогу по поводу его потенциального неправомерного использования негосударственными вооруженными группами и/или террористическими организациями, которые могут применять системы ИИ в целях планирования, координирования или осуществления атак. Эта угроза указывает на настоятельную необходимость в четко определенных, основанных на соблюдении прав человека законодательных мерах как на национальном, так и на международном уровнях.

Неотложность решения проблем, связанных с применением ИИ в террористических целях и в контртеррористической деятельности, была особо подчеркнута в ходе [Четвертого парламентского политического диалога](#), состоявшегося в Риме 5 декабря 2024 года. В ходе этого диалога, организованного [Программным офисом КТУ ООН по парламентскому взаимодействию](#) в сотрудничестве с [Парламентской ассамблеей ОБСЕ](#), была выявлена широко распространенная среди парламентариев обеспокоенность по поводу отсутствия адекватной законодательной базы для регулирования использования ИИ и новых технологий в усилиях по противодействию терроризму и одновременного предотвращения их использования террористическими группами. Участники призвали к расширению сотрудничества и технической поддержки в целях устранения этих пробелов в регулировании и обеспечения соответствия международным правовым стандартам.

В этой связи Программный офис КТУ ООН по парламентскому взаимодействию, выступающий в качестве специализированного центра в системе Организации Объединенных Наций, в чьи задачи входит поддержка парламентских мер по противодействию терроризму и предотвращению насильственного экстремизма, активно участвует в определении приоритетных направлений, где требуется техническая помощь. В роли Секретариата [Координационного механизма парламентских ассамблей по противодействию терроризму](#) Программный офис регулярно проводит консультации с партнерскими ассамблеями в целях оценки меняющихся потребностей. Недавно проведенный опрос участников Механизма подтвердил, что управление новыми технологиями и в частности искусственным интеллектом является одной из главных проблем, которые требуют скоординированных ответных мер.

На этом фоне возникла очевидная потребность в создании специализированной многосторонней платформы, в рамках которой законодатели и эксперты могли бы изучать новые риски, связанные с использованием искусственного интеллекта в террористических целях и в контртеррористической деятельности. Такая платформа позволила бы обмениваться опытом разработки законодательства, углублять взаимное понимание проблем, возникающих в связи с быстро развивающимися технологиями, и содействовать выработке согласованных и основанных на уважении прав человека ответных мер в правовом поле. Конференция была предложена в ответ на эту потребность в целях поддержания диалога, содействия гармонизации законодательства и изучения путей международного сотрудничества в решении этого насущного и комплексной проблемы.

3. ВАЖНЕЙШИЕ ОБСУЖДЕНИЯ ПО ТЕМАТИЧЕСКИМ НАПРАВЛЕНИЯМ

3.1. Точки зрения и усилия парламентов

Основная часть Конференции была посвящена выступлениям международных парламентских ассамблей, участвующих в Координационном механизме парламентских ассамблей по противодействию терроризму. В этих докладах были представлены точки зрения и усилия региональных парламентов по предотвращению терроризма и противодействию ему, при этом особое внимание уделялось законодательным мерам в целях регулирования ИИ и новых технологий. Докладчики делились национальным и региональным опытом, рассуждая о растущей роли национальных парламентов и парламентских ассамблей в содействии разработке политических рамок, основанных на соблюдении прав человека и учитывающих соображения безопасности.

В нескольких докладах были приведены конкретные примеры активных мер, принимаемых парламентскими ассамблеями в ответ на угрозы в сфере безопасности, создаваемые новыми технологиями. Среди выступлений, которые хотелось бы особо отметить, были доклады ПАС, ПА ОБСЕ, МПА СНГ, ПАЧЭС и ТЮРКПА, в ходе которых были представлены различные законодательные подходы и практические инициативы.

ПАС подчеркнула важнейшую роль парламентов в решении проблемы неправомерного использования ИИ и новых технологий террористами и преступниками. ПАС представила свои усилия и усилия нескольких своих государств-членов, таких как Алжир, Саудовская Аравия и ОАЭ, по приведению законодательных и этических рамок в соответствие с международным правом и принципами защиты основных прав. Флагманские инициативы ПАС включают в себя работу [Центра глобальных исследований \(CGS\) ПАС](#), который опубликовал совместный доклад с Исполнительным директором Контртеррористического комитета (ИДКТК) Совета Безопасности ООН о [злонамеренном использовании ИИ и новых технологий террористами и преступными группировками](#). Этот доклад стимулировал создание *Глобального постоянного парламентского наблюдательного комитета по неправомерному использованию ИИ и ИКТ* со штаб-квартирой в Сан-Марино, который выпускает ежедневный дайджест актуальных событий в этой сфере.

Сотрудничество ПАС с ИДКТК продолжается в рамках рецензируемого исследовательского проекта под названием *Spyware Misuse: Legislative, Governance, and Judicial Considerations, Historical Evolution, and Technical Insights* («Неправомерное использование шпионского ПО: законодательные, управленческие и правовые соображения, историческая эволюция и технические идеи»), который, как ожидается, будет представлен на 80-й сессии Генеральной Ассамблеи ООН. Кроме того, ПАС поддерживает возглавляемый ООН консультативный процесс по созданию *Независимой международной научной группы экспертов по ИИ*, целью которой является совершенствование управления на глобальном уровне и углубление понимания рисков, связанных с ИИ. ПАС также сообщила о своей текущей работе над [Валлеттскими принципами разработки национальных и региональных контртеррористических стратегий](#), представленными в ходе онлайн-семинара 9 мая после встречи под эгидой ООН на Мальте.

[Резолюция Парламентской ассамблеи ОБСЕ об искусственном интеллекте и борьбе с терроризмом](#), принятая в Бухаресте в июне 2024 года, также была представлена в качестве важнейшего международного ориентира в решении проблемы двойного назначения ИИ. ПА ОБСЕ подчеркнула описанный в резолюции сбалансированный подход, направленный на содействие использованию ИИ в контртеррористической деятельности при одновременной защите прав человека и основных свобод и гарантии верховенства права. Резолюция призывает к укреплению правовых рамок, надежным этическим стандартам и эффективным механизмам надзора. Кроме того, в ней пропагандируются государственно-частное партнерство, обязательная маркировка контента, сгенерированного ИИ, и инициативы по повышению уровня медиаграмотности в целях повышения устойчивости общества.

Продолжающиеся усилия ПА ОБСЕ по применению на практике положений резолюции были отмечены в ходе *Четвертого парламентского политического диалога*, который состоялся в Риме в декабре 2024 года. ПА ОБСЕ также упомянула об участии своего [Специального комитета по противодействию терроризму](#) в работе ведущих глобальных платформ, включая Форум по управлению Интернетом в Эр-Рияде, а также официальные

визиты в Турцию, которые способствовали обмену передовым опытом и укреплению многостороннего сотрудничества. Эти инициативы подчеркнули приверженность ПА ОБСЕ проактивному и основанному на соблюдении прав человека подходу к противодействию угрозам безопасности, связанным с ИИ.

В своих выступлениях представители МПА СНГ подчеркнули внесенный ими вклад в законодательную деятельность по управлению ИИ и противодействию терроризму. Особое внимание было уделено принятому в апреле 2025 года [модельному закону «О технологиях искусственного интеллекта»](#), разработанному совместно с Объединенным институтом проблем информатики Национальной академии наук Беларуси. Этот модельный закон обеспечивает всеобъемлющую правовую и этическую основу для безопасного развития и применения ИИ в странах СНГ. Он призывает к использованию общей терминологии, интеграции ИИ в ключевые отрасли при поддержке государства и проведение оценки воздействия технологий в законодательные процессы. Эта инициатива согласуется с повестками дня Генеральной Ассамблеи Организации Объединенных Наций и Международного союза электросвязи.

Параллельно с этим МПА СНГ завершает работу над *модельным законом «О противодействии использованию автономных и роботизированных систем в террористических и экстремистских целях»*, который разрабатывается в ответ на растущий риск применения технологий на основе ИИ в злонамеренных целях. Представители подчеркнули необходимость создания четких правовых механизмов для привлечения к ответственности как разработчиков систем, так и конечных пользователей, особенно в связи с постоянным повышением доступности автономных технологий. Эти усилия отражают более общую приверженность МПА СНГ распространению передовой международной и региональной парламентской практики в области регулирования ИИ. Представители отметили, что парламентские ассамблеи располагают выгодными возможностями для содействия применению этой практики в других регионах, способствуя межпарламентскому сотрудничеству, обмену передовым опытом и гармонизации правовых мер, принимаемых в ответ на угрозы безопасности, связанные с ИИ.

Парламентская ассамблея Черноморского экономического сотрудничества (ПАЧЭС) указала на растущую международную значимость искусственного интеллекта и новых технологий в сфере противодействия терроризму. Ассамблея подчеркнула, что в связи с усложнением угроз безопасности необходимо всеобъемлющее законодательство, учитывающее двойное назначение этих технологий. ПАЧЭС подчеркнула важность принятия мер к тому, чтобы правовые рамки были ориентированы на перспективу и обеспечивали баланс между технологическими инновациями и защитой прав человека и основных свобод.

В представленном докладе ПАЧЭС отметила свое намерение продолжать изучение потенциала ИИ в ходе предстоящих обсуждений в рамках работы своих комитетов, особенно вопросов, касающихся его применения в целях устойчивого социально-экономического развития. Ассамблея признала, что законодательные меры, регулирующие

ИИ, должны быть направлены не только на снижение рисков, но и на признание возможностей, которые ИИ предоставляет при ответственном применении в целях противодействия терроризму. Ассамблея вновь подтвердила необходимость регионального сотрудничества в разработке гармонизированных правовых стандартов, отражающих как потребности в сфере безопасности, так и демократические ценности.

Парламентская ассамблея тюркских государств (ТЮРКПА) подчеркнула настоятельную необходимость принятия согласованных законодательных мер в ответ на растущую угрозу, создаваемую искусственным интеллектом и другими новыми технологиями в случае их неправомерного использования террористами. ТЮРКПА предупредила, что в отсутствие регулирования такие технологии могут расширять возможности террористических организаций в таких областях, как распространение пропаганды, шифрование связи и кибератаки. Ассамблея особо указала на необходимость разработки эффективных правовых рамок в целях обеспечения прозрачности, этического регулирования и полного соответствия ИИ-систем стандартам в области прав человека.

ТЮРКПА призвала к разработке общих международных норм, способствующих трансграничному сотрудничеству, обмену информацией и установлению стандартов с целью противодействия связанным с ИИ угрозам безопасности, имеющим транснациональный характер. Ассамблея высказалась в поддержку более тесного сотрудничества между технологическими компаниями и государственными учреждениями в целях совершенствования механизмов раннего предупреждения, инфраструктуры кибербезопасности и информирования общественности. Она подчеркнула, что в предотвращении неправомерного использования новых технологий и укреплении устойчивости общества ведущую роль играют просвещение общественности о рисках и преимуществах ИИ в сочетании с четкими нормативными требованиями. В заключение ТЮРКПА отметила, что для обеспечения общественной безопасности и поддержания верховенства права в цифровую эпоху необходима разработка гармонизированных правовых рамок как на национальном, так и на международном уровнях.

3.2. Международные организации, стандарты и правовые рамки

После докладов, представляющих точки зрения парламентов, делегаты от международных организаций поделились своими взглядами на соответствующие международные стандарты, правовые рамки и меры, относящиеся к необходимым законодательным и нормативным мерам противодействия использованию ИИ и других новых технологий в террористической деятельности.

Международный комитет Красного Креста (МККК) подчеркнул, что расширение использования ИИ в усилиях по противодействию терроризму порождает неотложные и комплексные гуманитарные проблемы. Будучи нейтральной, независимой и беспристрастной гуманитарной организацией, работающей в условиях вооруженных конфликтов и других ситуациях применения насилия, МККК на собственном опыте убедился в том, как новые технологии, применяемые без надлежащих защитных мер,

повышают риски для гражданского населения, затрудняют доступ гуманитарных работников и влияют на принятие решений, касающихся жизни и смерти. МККК отметил, что использование технологий ИИ в автономных вооружениях и военных системах поддержки принятия решений может вызвать серьезные правовые, этические и оперативные проблемы.

МККК подчеркнул, что ИИ по своей сути не является хорошей или плохой технологией, но предоставляет набор инструментов, которые необходимо использовать ответственно. Несмотря на то, что сам МККК использует ИИ и цифровые технологии в целях повышения эффективности своей деятельности в таких областях, как логистика и здравоохранение, он особо указал на необходимость эффективного внутреннего контроля, технических знаний и превентивного подхода к управлению рисками. Он также выразил обеспокоенность по поводу потенциального неправомерного использования ИИ хакерами, в том числе замышляющими кибератаки на гуманитарные организации.

С правовой и этической точек зрения МККК призвал к интеграции гуманитарных защитных мер в национальные и международные законодательные и нормативные рамки. В докладе указывалось, что ответные меры, касающиеся использования ИИ в усилиях по противодействию терроризму, должны выходить за рамки решения неотложных задач в сфере безопасности и ставить во главу угла человеческое достоинство, подотчетность и соблюдение норм [международного гуманитарного права \(МГП\)](#). МККК отметил, что во всех процессах принятия решений с помощью ИИ главное место должно отводиться человеческому здравому смыслу. Машины не в состоянии принять на себя юридическую ответственность, возложенную на людей, особенно в вооруженных конфликтах, когда необходимо четко и прозрачно принимать решения на основе правовой позиции в соответствии с МГП.

МККК выразил особую обеспокоенность в связи с тем, что системы с технологиями ИИ потенциально подкрепляют предвзятость, генерируют ошибки и маскируют подотчетность ввиду своего комплексного характера и недостатка прозрачности. Он указал на риски предвзятости, связанные с автоматизацией, когда чрезмерная зависимость от предлагаемых машиной результатов может превратить лиц, принимающих решения, из ответственных уполномоченных в пассивных исполнителей. В целях снижения этих рисков он призвал к реальному контролю со стороны человека, надежным механизмам надзора и разработке новых обязательных международных правил в отношении автономных систем вооружений, особенно характеризующихся непредсказуемым поведением или предназначенных для непосредственной атаки на людей.

МККК предупредил, что меры по противодействию терроризму, разрабатываемые на основе технологий ИИ без учета норм международного права, могут повлечь непреднамеренные негативные последствия для гуманитарной деятельности и населения, нуждающегося в защите. Он приветствовал [резолюции 2462](#) и [2482](#) Совета Безопасности, в которых признаются эти риски и содержится призыв к государствам соблюдать МГП. МККК решительно выступил в поддержку введения специальных исключений для

гуманитарных организаций в политику об антитеррористических мерах, касающихся использования ИИ, чтобы такие меры не мешали беспристрастной гуманитарной деятельности.

В заключение МККК призвал государства и парламенты принять меры к тому, чтобы законодательные и политические рамки, регулирующие применение ИИ в усилиях по противодействию терроризму, отражали обязательства по МГП, предусматривали механизмы подотчетности и прозрачности и разрабатывались в рамках инклюзивного диалога с участием множества заинтересованных сторон. Был выражен призыв, в частности к парламентам, взять на себя ведущую роль в том, чтобы не допустить попрания основных прав и средств защиты в условиях стремительного технологического прогресса. Если при принятии политических решений во главу угла ставятся люди, особенно подвергающиеся наибольшему риску, то ИИ будет не только служить инструментом обеспечения безопасности, но нести пользу для человечества.

Программный офис КТУ ООН по парламентскому взаимодействию в сфере предотвращения терроризма и противодействия ему подчеркнул, что, хотя искусственный интеллект и другие новые технологии открывают новые возможности для усиления контртеррористических мер, их неправомерное использование террористами вызывает серьезные проблемы с правовой и этической точек зрения и в сфере безопасности. Для решения этих проблем требуются своевременные, скоординированные и ориентированные на перспективу законодательные меры как на национальном, так и на международном уровнях.

Опираясь на итоги *Четвертого парламентского политического диалога*, состоявшегося в Риме в декабре 2024 года, Программный офис отметил, что Конференция служит важнейшей платформой для изучения последствий применения ИИ и других новых технологий в террористических целях. Ее целью является выявление пробелов в существующих правовых рамках, обмен передовым опытом и деятельность по разработке модельной правовой базы, в которой были бы сбалансированы технологические инновации, неотложные задачи в сфере безопасности и защита прав человека.

Программный офис также описал свои более общие усилия по содействию инклюзивным законодательным подходам, основанным на соблюдении прав человека, в том числе пояснил свои функции как Секретариата Координационного механизма парламентских ассамблей по противодействию терроризму. В этой роли он стимулирует устойчивый межпарламентский диалог, содействует гармонизации правовых норм и поощряет обмен знаниями и передовым опытом между парламентскими ассамблеями по всему миру. Программный офис подтвердил свою приверженность продвижению практически реализуемых совместных решений, основанных на нормах международного права и соответствующих основным принципам в области прав человека.

Программный офис КТУ ООН по парламентскому взаимодействию подчеркнул, что стремительное развитие искусственного интеллекта и других новых технологий как

открыло многообещающие возможности, так и породило серьезные проблемы для глобальной контртеррористической деятельности. Признавая сложные правовые, этические и гуманитарные проблемы, которые возникают в связи с этими технологиями, особенно их потенциальное неправомерное использование террористами и соответствующие риски, Программный офис активно работает над повышением осведомленности национальных парламентов и парламентских ассамблей по всему миру. Его усилия сосредоточены на привлечении внимания к широкому спектру вопросов, проблем и возможностей, которые предлагают ИИ и новые технологии, и одновременном распространении практически реализуемых законодательных и политических решений, основанных на соблюдении прав человека и соответствующих международным стандартам и передовой практике.

Отдел кибербезопасности и новых технологий Контртеррористического центра ООН при Контртеррористическом управлении Организации Объединенных Наций (КТЦ ООН / КТУ ООН) представил подробный обзор рисков и сложностей в нормативной сфере, связанных с использованием ИИ в террористических целях. Было отмечено, что к технологиям ИИ относятся самые разнообразные системы, разработанные в целях моделирования различных аспектов человеческого интеллекта, включая анализ данных, распознавание образов и автоматизированное принятие решений, и, хотя у таких технологий многообещающие перспективы, они также представляют серьезные риски в случае их использования террористами. Ссылаясь на Новую повестку дня в области мира, опубликованную Генеральным секретарем ООН в июле 2023 года, особое внимание в докладе было уделено тому, что растущая мощь и доступность генеративного ИИ порождает все больше угроз политической стабильности, общественному доверию и безопасности гражданского населения, как, например создание дипфейков.

Были освещены основные выводы совместного доклада КТЦ ООН / КТУ ООН и ЮНИКРИ о злонамеренном использовании искусственного интеллекта в террористических целях, в том числе определены разнообразные угрозы, связанные с использованием ИИ, включая более изощренные кибератаки, автономные системы вооружений, кампании по дезинформации и биоинженерное оружие. Эти проблемы подчеркивают настоятельную необходимость разработки нормативно-правовой базы, которая предусматривала бы защитные меры, учитывающие гуманитарные факторы и направленные на защиту прав человека, в соответствии с актуальными резолюциями ООН, такими как резолюции 2178, 2370 и 2396 Совета Безопасности, Мадридские руководящие принципы и Делийская декларация.

В целях содействия государствам-членам в борьбе с этими угрозами в докладе был представлен ряд инициатив КТУ ООН. К ним относятся программа *Cybersecurity and New Technologies* («Кибербезопасность и новые технологии»), направленная на наращивание потенциала и устойчивости к террористическим кибератакам на критически важную инфраструктуру, а также инициативы СТ ТЕСН и СТ ТЕСН+, разработанные в рамках этой программы в партнерстве с Интерполом при финансировании Европейского союза и направленные на укрепление потенциала государств-членов в противодействии

неправомерному использованию террористами новых и новейших технологий путем предоставления правоохранительным органам и работникам системы уголовного правосудия поддержки, основанной на соблюдении прав человека, учитывающей гендерные аспекты и ориентированной на оперативную ситуацию. Программа также предусматривает наращивание потенциала в таких областях, как искусственный интеллект, расследования по открытым источникам, расследования в даркнете и цифровая криминалистика.

В заключение доклада прозвучал призыв к применению скоординированных, основанных на соблюдении прав человека подходов к управлению ИИ, с акцентом на то, что ИИ не только представляет собой технологический инструмент, но и подразумевает этическую ответственность и здравомыслие. Также было указано на то, что законодательные и нормативные меры должны эволюционировать параллельно с технологическим прогрессом, чтобы эффективно предотвращать неправомерное использование ИИ террористами. Такие меры должны четко определять границы допустимого использования, обеспечивать надзор и подотчетность, а также соответствовать нормам международного права, включая международное гуманитарное право и право в области прав человека. Для принятия эффективных ответных мер потребуются тесное сотрудничество между правительствами, субъектами частного сектора и гражданским обществом, с тем чтобы ИИ служил миру и безопасности, а не усугублял угрозы.

Исполнительный директорат Контртеррористического комитета (ИДКТК) указал на растущую важность разработки ответственной и эффективной законодательной и нормативной базы, направленной на решение проблемы использования искусственного интеллекта в террористических целях. В рамках своего мандата, определенного Советом Безопасности, ИДКТК проводит техническую оценку выполнения государствами-членами обязательств по противодействию терроризму и координирует оказание технической помощи. В ходе этой работы ИДКТК выявил несколько новых практических подходов, касающихся ИИ, включая принцип обеспечения безопасности на стадии проектирования, программирование с учетом этических стандартов, оценку воздействия и инициативы в области цифровой грамотности, направленные на повышение устойчивости общества в отношении контента и сбора средств с использованием технологий ИИ в террористических целях.

ИДКТК подчеркнул, что при разработке парламентариями законодательных мер в ответ на террористические угрозы, связанные с искусственным интеллектом, крайне важно не изобретать велосипед. Многочисленные структуры, инициативы и правовые документы, такие как [Глобальный цифровой договор Организации Объединенных Наций](#), [Руководство АСЕАН по управлению ИИ и этике его применения](#), а также резолюции ПАС, уже заложили прочную основу. Вместо того, чтобы разрабатывать новые законы с нуля, ИДКТК рекомендовал пересмотреть и внести поправки в существующее национальное законодательство, чтобы учесть возможность использования цифровых технологий и технологий искусственного интеллекта в террористических целях. Например, можно дополнить существующие законы, касающиеся традиционной пропаганды или вербовки,

чтобы включить в них положения о противодействии распространению цифрового контента.

Важно отметить, что, согласно рекомендации ИДКТК, законодательство должно регулировать не только то, как негосударственные субъекты используют ИИ в террористических целях, но и то, как государства применяют ИИ в усилиях по противодействию терроризму, в том числе в целях слежки, сбора цифровых доказательств и в следственной практике. Такие сценарии использования должны соответствовать нормам международного права, в частности международного права в области прав человека и гуманитарного права, чтобы не допустить превышения полномочий, защитить неприкосновенность частной жизни и обеспечить выполнение надлежащих правовых процедур. Было подчеркнуто, что для прогнозирования и смягчения потенциальных непредвиденных последствий важное значение имеет разработка подходов к оценке соблюдения прав человека, в том числе с учетом гендерных аспектов.

Кроме того, ИДКТК выступал за подход к разработке законодательства, основанный на участии всего общества, поощряя инклюзивное взаимодействие с заинтересованными сторонами, общественные консультации и государственно-частное партнерство в целях обеспечения того, чтобы нормативные акты, регулирующие ИИ, были всеобъемлющими, технологически обоснованными и адаптируемыми к будущим разработкам. Особое внимание было уделено необходимости гармонизации законодательства на международном уровне для решения юрисдикционных проблем, возникающих в связи с трансграничным характером цифрового терроризма. В заключение ИДКТК подтвердил важнейшую роль парламентариев в создании эффективных, инклюзивных и основанных на соблюдении прав человека механизмов противодействия терроризму и выразил готовность оказывать поддержку государствам-членам в выработке решений, которые были бы эффективными и устойчивыми.

3.3. Сектор безопасности и правоохранительная деятельность

Участие представителей международных и региональных учреждений и организаций, занятых в сфере безопасности, обогатило дискуссию и углубило понимание многогранных вопросов, связанных с применением ИИ и новых технологий в усилиях по противодействию терроризму. В выступлениях представителей Антитеррористического центра Содружества независимых государств (АТЦ СНГ), его Научно-консультативного совета и различных руководителей АТЦ СНГ был представлен всесторонний региональный взгляд на правовые, оперативные и стратегические аспекты.

АТЦ СНГ подчеркнул растущую угрозу, которую представляет собой неправомерное использование ИИ и новых технологий в террористических целях, и призвал к усилению региональных правовых ответных мер. На фоне геополитической нестабильности и ослабления международных институтов АТЦ СНГ подчеркнул важность расширения евразийской правовой интеграции и совместной законодательной деятельности государств — участников СНГ. Центр внес существенный вклад в разработку

и совершенствование модельных законов в рамках работы МПА СНГ, в частности в таких сферах, как национальная безопасность, киберпреступность, безопасность границ и противодействие терроризму.

Особое внимание было уделено проекту модельного закона СНГ «*О противодействии использованию автономных и роботизированных систем в террористических и экстремистских целях*», разработанному в рамках Программы сотрудничества государств — участников СНГ в сфере борьбы с терроризмом и иными насильственными проявлениями экстремизма на 2023–2025 годы. Эта инициатива направлена на решение проблемы отсутствия точных юридических определений и гармонизированных стандартов для автономных систем. Она опирается на ряд региональных и международных источников, включая Заявление глав государств СНГ о развитии искусственного интеллекта гражданского назначения, Казанскую декларацию, рекомендации [Парламентской ассамблеи ОДКБ](#) и Концепцию безопасности Союзного государства. Законопроект призван привести новые технологии в соответствие с приоритетами в сфере безопасности и одновременно обеспечить правовую согласованность с модельным законом СНГ «*О технологиях искусственного интеллекта*».

АТЦ СНГ также внесла свой вклад в разработку проекта модельного закона «*Об общественной безопасности*», который, как ожидается, будет принят МПА СНГ в ближайшее время. Это позволит подготовить подробные комментарии в целях содействия его внедрения на законодательном уровне. На перспективу АТЦ СНГ изучает возможности разработки других типовых правовых актов в области национальной безопасности, химического терроризма, оперативно-розыскных мероприятий и интеграции норм международного гуманитарного права в региональные ответные меры, касающиеся автономных систем. Центр отметил продуктивное сотрудничество с Региональной антитеррористической структурой Шанхайской организации сотрудничества (РАТС ШОС) и объявил о планах провести последующее мероприятие в Душанбе (Таджикистан) в конце этого года.

В заключение АТЦ СНГ высказался за институционализацию ежегодных совместных антитеррористических конференций и предложил включить обсуждаемые законодательные инициативы в очередное решение Совета МПА СНГ. Центр вновь подтвердил свое обязательство содействовать гармонизации правовой базы в рамках скоординированного сотрудничества.

Дополняя это выступление, Научно-консультативный совет при АТЦ СНГ подчеркнул необходимость принятия решительных научных и правовых мер в ответ на активное использование ИИ в террористической деятельности. Последние статистические данные по регионам свидетельствуют о значительной концентрации преступлений, связанных с терроризмом, в странах СНГ, что требует внимания со стороны регулирующих органов к ИИ, беспилотным системам, робототехнике и цифровому финансированию.

Совет обратил внимание на риски, присущие технологиям ИИ, в том числе на их двойное назначение, непрозрачность и расширяющуюся автономность. Эти риски выходят за рамки угроз безопасности и затрагивают более широкие социальные проблемы, такие как дезинформация, социальная изоляция, потеря автономии и негативное воздействие на психическое здоровье и развитие детей. Распространение дипфейков, пропаганда на основе ИИ и такие системы, как *Oculus*, предназначенные для обнаружения незаконного контента, демонстрируют двойной характер применения ИИ в информационном пространстве.

Совет призвал к гармонизации правовых норм в техническом, этическом и правовом аспектах. Он приветствовал сделанное в 2024 году Заявление глав государств СНГ о сотрудничестве о развитии искусственного интеллекта гражданского назначения, в котором содержится призыв к государственному надзору, надежной цифровой инфраструктуре и центральной координирующей роли ООН в глобальном управлении ИИ. Совет также подчеркнул необходимость определения ограничений на использование ИИ в контексте национальной безопасности, наряду с механизмами тестирования, проверки достоверности и подотчетности.

Важнейшими правовым документом были признаны Рекомендации МПА СНГ по нормативному регулированию использования искусственного интеллекта, в частности по причине их особого внимания к этическим стандартам, направленным против манипуляций и дискриминации. Положительно были отмечены недавние законодательные инициативы, в том числе поправки в уголовном праве, которые относят использование ИИ котягающим факторам. Совет также призвал к развитию криминологического прогнозирования, защите от неправомерного использования биометрических данных и совершенствованию технологий идентификации для пограничного и миграционного контроля.

В своем заключительном слове Совет призвал к созданию всеобъемлющего правового и этического режима для предотвращения использования ИИ в террористических целях. Он высказался в поддержку сбалансированного подхода, сочетающего общие ограничения с целевыми нормами и подкрепленного информированием общественности, цифровой грамотностью, проверкой фактов и защитными мерами для достижения цифрового суверенитета.

Выступившие руководители АТЦ СНГ приветствовали Конференцию как своевременную инициативу в ответ на стремительно меняющийся профиль угроз. Они признали 25-летнее наследие совместных усилий СНГ по противодействию терроризму и отметили, что нестабильность в таких регионах, как Афганистан и Ближний Восток, продолжает подпитывать радикальные направления идеологии, нацеленные на молодежь и уязвимые слои населения.

Руководители Центра отметили, что террористические группы все чаще используют ИИ и цифровые технологии в целях пропаганды, вербовки, шифрования связи, координирования атак и получения финансирования. В качестве серьезной угрозы,

требующей незамедлительного внимания со стороны регулирующих органов, были определены производство убедительного фейкового контента с помощью технологий ИИ и его распространение. Эти темы уже рассматривались в рамках дискуссий МПА СНГ по вопросам общественной безопасности и дерадикализации.

В ходе своих выступлений эксперты подтвердили намерение АТЦ СНГ обеспечить при разработке регионального законодательства соответствие международным стандартам. Была выражена заинтересованность в расширении взаимодействия с КТУ ООН, в частности, в рамках его межпарламентских инициатив, таких как предстоящий Контртеррористический форум в Душанбе.

Затрагивая перспективы, АТЦ СНГ подчеркнул свою роль в составлении следующего Перспективного плана модельного законодательства в СНГ, подтвердив свою приверженность повышению эффективности коллективных ответных мер в рамках сотрудничества с МПА СНГ и международными партнерами. В заключение Центр подчеркнул важность международного сотрудничества в правовой сфере в целях обеспечения безопасности, гармонизации правовых рамок и повышения устойчивости перед лицом террористических угроз, связанных с использованием ИИ.

3.4. Компании частного сектора, научно-исследовательские центры и академические учреждения

Участие представителей частного сектора, академических учреждений и исследовательских центров обогатило Конференцию ценными точками зрения. В их выступлениях подчеркивалась важная роль, которую технологические инновации, междисциплинарные исследования и межотраслевое сотрудничество играют в противодействии растущим рискам, связанным с неправомерным использованием ИИ и новых технологий в террористических целях.

В ходе обсуждений особо упоминалось, что технологии ИИ разрабатываются и внедряются слишком быстрыми темпами, зачастую опережая существующую нормативно-правовую базу, что указывает как на перспективы технологического прогресса, так и проблемы, которые он создает. Участники отметили необходимость укрепления партнерских отношений между государственным сектором и частными компаниями, с тем чтобы обеспечить разработку и использование ИИ на основе безопасных и этических подходов, соответствующих принципам соблюдения прав человека.

Научно-исследовательские центры подчеркнули важность комплексной оценки рисков, внедрения принципов обеспечения безопасности на стадии проектирования и применения технических защитных мер в целях предотвращения неправомерного использования ИИ. Они обозначили необходимость повышения прозрачности алгоритмов, более строгого управления данными и создания механизмов подотчетности для укрепления доверия к системам с технологиями ИИ и повышения устойчивости.

Академические учреждения также подчеркнули важность междисциплинарного образования и обучения, с тем чтобы будущие эксперты приобрели компетенции, необходимые для успешного преодоления последствий, связанных с новыми технологиями, в социальной и правовой сфере, а также в сфере безопасности. В качестве важнейшего шага на пути к ответственным инновациям была определена разработка учебных программ, сочетающих технические знания с пониманием этических стандартов.

Представители компаний частного сектора подчеркнули, что, несмотря на свою ведущую роль в развитии ИИ, они также несут ответственность за прогнозирование и смягчение потенциальных угроз, возникающих в результате его неправомерного использования. Представители отрасли высказывались за расширение сотрудничества и обмена информацией с директивными и регулируемыми органами и гражданским обществом в целях обеспечения того, чтобы системы различного назначения с технологиями ИИ способствовали коллективной безопасности.

Выступавшие коллективно признали важнейшую роль адекватного законодательства и регулирования в поддержке безопасной и ответственной инновационной среды. Эффективная правовая база обеспечит понятные требования, стимулы и механизмы защиты, необходимые компаниям частного сектора, научно-исследовательским центрам и ученым для ответственной работы, и одновременно поможет в снижении рисков. Директивным органам было рекомендовано поддерживать тесное взаимодействие с техническими и отраслевыми экспертами в целях дальнейшего обеспечения адаптивности и эффективности законодательства и его соответствия международным стандартам.

В заключение участники еще раз подтвердили, что для предотвращения использования ИИ и новых технологий в террористических целях требуется подход, основанный на участии всего общества. Вклад компаний частного сектора, академических учреждений и научно-исследовательских сообществ необходим для выработки гибких и ориентированных на перспективу стратегий. Их активное участие имеет решающее значение в обеспечении того, чтобы технологический прогресс направлялся этической дальновидностью, инклюзивностью и непоколебимой приверженностью безопасности человека.

4. ОСНОВНЫЕ ВЫВОДЫ, РЕКОМЕНДАЦИИ И ПОСЛЕДУЮЩИЕ МЕРЫ

Участники Конференции подчеркнули укрепление консенсуса среди парламентариев, международных организаций, гуманитарных организаций и технических экспертов в отношении неотложности решения проблемы двойного назначения искусственного интеллекта и новых технологий с точки зрения их применения в террористических целях и в контртеррористической деятельности. Участники коллективно признали, что, хотя ИИ обладает значительным потенциалом повышения эффективности операций по обеспечению безопасности, его неправомерное использование террористами создает беспрецедентные правовые, этические и оперативные проблемы, требующие своевременных, инклюзивных и скоординированных ответных мер.

Одним из наиболее важных результатов Конференции стали значительные пробелы, выявленные в существующих национальных и международных правовых базах в отношении использования и регулирования ИИ в контртеррористической деятельности. Участники подчеркнули, что технологический прогресс идет настолько быстрыми темпами, что опережает действующее законодательство, а это, в свою очередь, ведет к появлению «слепых зон» в регулировании и несогласованных между собой стандартов в разных юрисдикциях. В целях решения этой проблемы в качестве одной из важнейших потребностей была отмечена разработка модельной законодательной базы, основанной на международном гуманитарном праве и международном праве в области прав человека. Такая законодательная база должна соответствовать нормам международного права и включать в себя принципы прозрачности, подотчетности, соразмерности, а также предусматривать надежные механизмы надзора.

Конференция также подчеркнула важность человекоориентированного подхода к управлению ИИ. В ходе обсуждений по всем тематическим направлениям участники подчеркнули, что человеческое здравомыслие и подотчетность должны оставаться в центре разработки, развертывания и использования технологий ИИ, особенно в случае угроз безопасности и гуманитарных ситуациях, характеризующихся высоким уровнем риска. Кроме того, особо указывалось на необходимость обеспечения конструктивного участия множества заинтересованных сторон, включая частный сектор, научно-академическую сферу и гражданское общество, как важнейшего фактора выработки целостных и ориентированных на перспективу решений.

На основе этих выводов были сформулированы следующие ключевые рекомендации:

- Поддержать разработку основанной на соблюдении прав человека и согласованной на международном уровне модельной правовой базы в целях регулирования использования ИИ и новых технологий в контртеррористической деятельности.
- Укреплять потенциал национальных парламентов в области законодательной деятельности и надзора за использованием ИИ и новых технологий, в том числе путем оказания технической помощи, экспертных консультаций и обмена опытом.
- Стимулировать межпарламентский диалог в целях содействия согласованию законодательных мер и обмену передовым опытом.
- Укреплять сотрудничество между национальными парламентами, правительствами, компаниями частного сектора и научно-исследовательскими сообществами в целях обеспечения баланса между инновациями и снижением рисков.
- Уделить приоритетное внимание введению специальных исключений и защитных мер для гуманитарных организаций в законодательство, направленное на противодействие терроризму, в целях обеспечения беспристрастной гуманитарной деятельности и защиты населения, находящегося в зоне риска.

- Содействовать информированию общественности, повышению цифровой грамотности и обеспечению прозрачности алгоритмов в целях снижения уязвимости и повышения устойчивости общества к угрозам, связанным с использованием ИИ.

В качестве конкретной последующей меры по итогам Конференции был подготовлен предварительный перечень совместных мероприятий, которые должны быть изучены Программным офисом КТУ ООН по парламентскому взаимодействию, МПА СНГ и МККК в тесном сотрудничестве с заинтересованными национальными парламентами. Эта деятельность включает в себя разработку типовых законодательных положений, семинары по наращиванию потенциала и тематические брифинги, призванные поддержать на национальном уровне внедрение эффективных, этичных и основанных на соблюдении прав норм регулирования использования ИИ в усилиях по противодействию терроризму.

5. ЗАКЛЮЧЕНИЕ

Конференция послужила своевременной и ориентированной на действия платформой для диалога, сотрудничества и стратегического размышления, направленной на решение одной из самых комплексных и быстро меняющихся задач в современной контртеррористической деятельности: регулирование искусственного интеллекта и других новых технологий. Она вновь подтвердила коллективное признание того, что обеспечение безопасности в эпоху ИИ требует не только технологической подготовленности, но и безусловного соблюдения норм международного права, управления на основе этических стандартов и институционального сотрудничества.

Обсуждения, проведенные в парламентском, институциональном и техническом направлениях, показали общую решимость перейти от осознания к действиям. Делегаты признали ограниченность существующей правовой базы и призвали к целенаправленным скоординированным усилиям по устранению этих пробелов с соблюдением принципов законности, подотчетности и соразмерности. Было выражено широкое согласие с тем, что парламентские институты призваны сыграть уникальную и незаменимую роль в этом процессе, учитывая их законодательные мандаты, надзорные функции и возможности для преодоления разрыва между глобальными нормами и их реализацией на национальном уровне.

Конференция завершилась призывом поддерживать и расширять партнерские отношения, установленные в рамках этого мероприятия. Участники выразили значительную заинтересованность в продолжении обмена знаниями и передовым опытом, продвижении законодательных решений и выработке единого подхода к противодействию неправомерному использованию ИИ в террористических целях. Благодаря совместным усилиям, обоснованной выработке политического курса и инклюзивному диалогу заинтересованные стороны взяли на себя обязательство обеспечить, чтобы в будущем при использовании новых технологий в контртеррористической деятельности соблюдались принципы защиты прав человека, гарантировалось верховенство права и поддерживались международный мир и безопасность.

6. КОММУНИКАЦИЯ

Пресс-релизы

https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/20250417_parliamentai_press_release_final.pdf

https://iacis.ru/novosti/partneri/mezhdunarodnaya_konferentciya_v_peterburge_kak_protivostoyat_ispolzovaniyu_ii_v_terroristicheskikh_tcelyah

<https://www.oscepa.org/en/news-a-media/news-from-copenhagen/2025/5210-news-from-copenhagen-1007/file>

<https://pam.int/pam-contributes-to-the-un-led-global-dialogue-on-legal-frameworks-to-address-the-misuse-of-ai-by-terrorist-groups/>

<https://www.pabsec.org/news-detail/participation-of-mr-asaf-hajiyev-pabsec-secretary-general-in-the-unoct-international-conference-st-petersburg-17-april-2025/720>

<https://turkpa.org/tr/news/1804-turkpa-participated-in-the-international-conference-on-counter-terrorism-in-st-petersburg>

<https://cisatc.org/1289/136/9138/9620>

Твиты

https://x.com/UN_OCT/status/1913069673156870350