**ӘОЖ 343.102:351.745.7**
**МҒТАР 10.71.43**

**М.Б. Садықов[1], А.А. Тынышбаева[2]**
*[1]Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясы, Қосшы қ., Қазақстан Республикасы*
*[2]Қазақстан Республикасы Президентінің жанындағы Мемлекеттік басқару академиясы, Астана қ., Қазақстан Республикасы*

# ТЕРРОРИЗМДІ БОЛЖАУ МЕН ОҒАН ҚАРСЫ КҮРЕСТЕ ЖАСАНДЫ ИНТЕЛЛЕКТТІ ҚОЛДАНУ: ХАЛЫҚАРАЛЫҚ ТӘЖІРИБЕГЕ ШОЛУ

**Аннотация.** Қазіргі тәжірибеге сүйене отырып, терроризмді болжауда және онымен күресте жасанды интеллекттің шешуші маңыздылығын байқауға болады. Бұл дағдарысқа қарсы шараларды қолдану әдістері мен дәрежесін анықтауда маңызды рөл атқарады. Бұл мақалада діни экстремизм мен терроризмді болжау мен оған қарсы күресте жасанды интеллектті қолданудың халықаралық тәжірибесі мен қазіргі жағдайы талданады, сонымен қатар DEXTER, Malicious use of artificial intelligence (MUAI), deepfake, Human intelligence (HUMINT) технологияларын және т.б. қолдану тәжірибесінің кейбір белгілі артықшылықтары мен кемшіліктері зерттеледі. Терроризмге қарсы күрес үшін технологияларды пайдалану процесінде шешілуін қажет ететін этикалық және моральдық мәселелерге назар аударылады. Мақаланың мақсаты-әлемдегі терроризмнің алдын алу және оған қарсы тұру үшін жасанды интеллектті қолданудың қазіргі жағдайы мен тәсілдеріне шолу.

**Түйінді сөздер:** жасанды интеллект; болжау; модель; құқықтар; MUAI; HUMINT; deepfake; DEXTER.

**М.Б. Садыков[1], А.А. Тынышбаева[2]**
*[1]Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, г. Косшы, Республика Казахстан*
*[2]Академия государственного управления при Президенте Республики Казахстан, г. Астана, Республика Казахстан*

# ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОГНОЗИРОВАНИИ И БОРЬБЕ С ТЕРРОРИЗМОМ: ОБЗОР МЕЖДУНАРОДНОЙ ПРАКТИКИ

**Аннотация.** Основываясь на современной практике, можно наблюдать решающее значение искусственного интеллекта в прогнозировании терроризма и борьбе с ним. Это играет жизненно важную роль в определении методов и степени применения антикризисных мер.

В данной статье анализируется международный опыт и текущее состояние использования искусственного интеллекта в прогнозировании и борьбе с терроризмом, а также исследуются некоторые известные преимущества и недостатки практики по применению DEXTER, Malicious use of artificial intelligence (MUAI), технологии deepfake, Human intelligence (HUMINT) и др. Обращается внимание на этические и моральные проблемы, которые необходимо решить, в процессе использования технологий для борьбы с терроризмом.

Целью статьи является обзор современного состояния и подходов к использованию искусственного интеллекта для предотвращения и борьбы с терроризмом в мире.

**Ключевые слова:** искусственный интеллект; прогнозирование; модель; права; MUAI; HUMINT; deepfake; DEXTER.

**M.B. Sadykov[1], A.A. Tynyshbayeva[2]**
*[1] Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, Kosshy c., Republic of Kazakhstan*
*[2]Academy of Public Administration under the President of the Republic of Kazakhstan, Astana c.,the Republic of Kazakhstan*

# THE USE OF ARTIFICIAL INTELLIGENCE IN FORECASTING AND COMBATING TERRORISM: OVERVIEW OF INTERNATIONAL PRACTICE

**Abstract.** Based on modern practice, one can observe the crucial importance of artificial intelligence in predicting terrorism and combating it. This plays a vital role in determining the methods and degree of application of anti-crisis measures. This article analyzes the international experience and the current state of the use of artificial intelligence in the forecasting and fight against terrorism, and also examines some of the known advantages and disadvantages of the practice of using DEXTER, Malicious use of artificial intelligence (MUAI), deepfake, Human intelligence (HUMINT) technologies, etc. In the process of using technologies to combat terrorism, attention is paid to ethical and moral issues that need to be addressed. The purpose of the article is to review the current state and approaches to the use of artificial intelligence to prevent and combat terrorism in the world.

**Keywords:** artificial intelligence; forecasting; model; rights; MUAI; HUMINT; deepfake; DEXTER.

DOI: 10.52425/25187252_2023_29_151

*Кіріспе.* Заманауи практика көрсеткендей, терроризмді болжау және оған қарсы күрес мақсатында жасанды интеллекттің рөлі қазіргі жағдайда дағдарысқа қарсы шаралардың қалай және қандай көлемде қолданатындығын анықтау шешуші мәнге ие.

Терроризмге қарсы күресте жасанды интеллектті қолдану, барлау қауымдастығының әртүрлі міндеттерді шешу үшін бірнеше жылдан бері жасанды интеллектті қолданып келе жатқанын көрсетеді. Атап айтқанда, жасанды интеллект пен машиналық оқытуға негізделген деректерді автоматтандырылған талдау қазірдің өзінде маңызды құрал болып табылады. Жасанды интеллект арнайы қызметтерге күдіктілерді тезірек анықтауға және басымдық беруге, күдіктілер арасындағы байланыстарды талдауға, тіпті арнайы қызмет назарындағы адамдарды бақылау үшін бет-әлпет пен дауысты тану технологияларын қолдануға мүмкіндік береді[1].

Мақаланың мақсаты-әлемдегі терроризмнің алдын алу және оған қарсы тұру үшін жасанды интеллектті қолданудың қазіргі жағдайы мен тәсілдеріне шолу.

*Материалдар мен әдістер.* Зерттеудің негізгі әдістері-сапалы бақылау, салыстырмалы-құқықтық талдау және әдебиеттерге шолу. Зерттеудің болжамды сипатын ескере отырып, этикалық-құқықтық модельдеу әдісі де қолданылады.

Қауіпсіздік саласында, жасанды интеллект мемлекеттік органдардың шегінен шығып, жеке компанияларға енеді. Олар өз жағынан платформаларын дұрыс пайдаланбау және дұшпандық мінез-құлық мониторингі үшін ұқсас модельдерді қолданады.

Қолдану практикасын талдау жасанды интеллект күрес стратегияларына айтарлықтай әсер ететінін көрсетеді [1, 139 б.]. Атап айтқанда, терроризмді болжауда, барлау және құқық қорғау қауымдастықтарына қатысы бар деп санауға болатын ықтимал қауіптерді анықтауда қолданылады. Осыған байланысты, терроризмге қарсы күрес тактикасы саласында жасанды интеллект зор мүмкіндіктерге ие. Бұл жасанды интеллекттің терроризмге қарсы стратегиясы ретіндегі ролі болашақта тек өседі деп болжауға мүмкіндік береді.

*Нәтижелер, талқылау.* Адамдар көп жиналатын жерлерде терроризммен күресу үшін НАТО жаңа технологияларды әзірледі. DEXTER (Detection of EXplosives and firearms to counter TERrorism) көмегімен

[1] The AI Revolution and Its Implications on Domestic Counterterrorism / Middlebury Institute of International Studies at Monterey, 2021 [Electronic resource] – Access mode: https://www.middlebury.edu/institute/academics/centers-initiatives/ctec/ctec-publications/ai-revolution-and-its-implications-domestic (Access data: 24.07.2023).

терроризммен күресу үшін жарылғыш заттар мен атыс қаруын анықтау арқылы адамдар көп жиналатын жерлерде атыс қаруы мен жарылғыш заттардан болатын қауіпке қарсы тұру үшін технологияның прототипі жасалды. DEXTER технологиясы қашықтықтан және нақты уақыт режимінде қозғалатын жаяу жүргіншілер арасында атыс қаруы мен жарылғыш заттарды тасымалдаушыларды анықтауға мүмкіндік береді [2, 76 б.].

Бұл бағытта ҚХР құқық қорғау жүйесінің жасанды интеллектті пайдалану тәжірибесі назар аударады. Бүкіл Қытайда полиция қылмыстар мен наразылықтарды олар болғанға дейін болжау үшін кең бақылау деректерін пайдаланады. Жүйелер мен бағдарламалық жасақтама, еш жамандық жасамаса да, алгоритм мен Қытай билігінің алдында мінез-құлқы немесе сипаттамалары күдікті адамдарға бағытталып отыр. Қытайда тұратын 1,4 миллиардтан астам адам тұрақты бақылауда. Оларды барлық жерде, көше бұрыштарында және метро төбелерінде, қонақүйлер мен көпқабатты үйлердің фойелерінде орналасқан полиция камералары түсіреді. Олардың телефондары, сатып алулары бақыланады, онлайн чаттар цензураға ұшырайды.

Соңғы буын технологиялары қылмыстар мен наразылықтарды олар болмай тұрып болжауға уәде беріп, заңдылықтар мен ауытқуларды табу үшін олардың күнделікті әрекеттері туралы жиналған көптеген деректерді қарастырады. Олар Қытай үкіметінің көзқарасы бойынша ықтимал құқық бұзушыларға – тек қылмыстық тарихы барларға ғана емес, сонымен қатар этникалық азшылықтарды, мигрант жұмысшыларды және психикалық аурулары бар адамдар сияқты осал топтарға да бағытталған[2].

Сонымен қатар бұрынғы уақытта тыңшылық және қадағалау технологиялары саласы негізінен мемлекеттік органдар мен штаттық техникалық сарапшылардың құзыреті болды. Алайда, қазіргі әлемде мемлекеттік құрылымдар қолданатын бақылау құралдарының басым көпшілігін жеке сектор компаниялары жеткізеді. Мұндай озық мүмкіндіктерді дамытатын жеке киберқауіпсіздік фирмаларының қатарына Израильден келген NSO, Quadream, Candiru және Saito Tech, Ұлыбританиядан келген Gamma International, Германиядан Vilicius Holding және Trovicor, Франциядан Qosmos және Amesys, area SpA және Италиядан келген Hacking Team/Memento Labs, cytrox кіреді. Венгрияда, Израиль мен Солтүстік Македония, сондай-ақ cyberpoint, Narus (Boeing еншілес компаниясы), Blue Coat Systems және Cisco Systems сияқты АҚШ компаниялары Біріккен Араб Әмірліктерінің DarkMatter-мен бірге. Адам құқықтарының бұзылуын болдырмау үшін осы кәсіпорындар мен көпұлтты корпорациялардың қызметін мемлекеттердің кәсіпкерлік секторды қадағалау жөніндегі міндеттеріне сәйкес реттеу жөнінде шұғыл шаралар қабылдау өте маңызды[3].

Жалпы бағалау кезінде қарастыруға тұрарлық жасанды интеллектті қолданатын қорғаныс құралдарының жалпы санаттарының бірі-терроризмге қарсы күресте жасанды интеллектті қолдану. Жасанды интеллект қазірдің өзінде бақылау камераларының адамның бет-әлпетін тану және әлеуметтік медианы талдау сияқты құқық қорғау мақсаттарының кең ауқымы үшін кең тарала бастады [3, 60 б.].

Агрессивті субъектілермен жасанды интеллектті зиянды қолдануынан (malicious use of artificial intelligence – MUAI) туындайтын халықаралық психологиялық қауіпсіздік саласындағы жаңа қауіптерге байланысты жасанды интеллекттің рөлі артып келеді. MUAI классификациясы жүзеге асушылыққа, аумақтық қамтуға, зақымдану дәрежесіне, таралу жылдамдығы мен формаларына, коммерциялық жасанды интеллект жүйелерін қайта бағдарлауға, «терең жалған» және жалған адамдарды құруға, манипуляциялық күн тәртібін құруға және

[2] NATO demonstrates new technology to counter terrorism in crowded venues / NATO, 2022 [Electronic resource] – Access mode: https://www.nato.int/cps/en/natohq/news_195801.htm (Access data: 24.07.2023).

[3] Fionnuala Ní Aoláin. Report of the Special Rapporteur on the on the promotion and protection of human rights and fundamental freedoms while countering terrorism. Human rights implications of the development, use and transfer of new technologies in the context of counter terrorism and countering and preventing violent extremism UN Doc. A/HRC/52/39. – 2023, p.15.

нығайтуға және болжамды қаруды қолдануға негізделген[4].

Террористік ұйымдардан таралатын MUAI қауіптерін анықтау үшін сценарийлік талдау қолданылады. Жасанды интеллект арқылы террористік актілердің ықтимал әсерін бағалау үшін IP-мекенжайы бойынша ықтимал террористік актілердің сценарийлері және олардың салдары қарастырылады, сондай-ақ алдын алу шаралары әзірленеді.

MUAI – Қазақстан үшін қауіпсіздік қатерлерімен байланысты жаңа халықаралық терроризмге қарсы іс-қимыл практикасы үшін аз зерттелген сала болып табылады. MUAI жасанды интеллектке қауіп-қатерді сапалы жаңа деңгейге көтереді, бұл қоғам тарапынан тиісті бағалау мен реакцияны қажет етеді. Жаңа қауіптерді түсіну процесі қазіргі әлемнің тез өзгеретін реалияларынан артта қалуда, ал жаңа қауіптердің саны тек арта түсетіні сөзсіз. Қоғамға зиян келтіру мақсатында, қоғамға жат субъектілер, соның ішінде террористік ұйымдар, тез таралатын және күннен күнге әзірлеудің құны төмендейтін жасанды интеллект жүйелерін қолдану ықтималдығы жоғары.

Мысалы, жасанды интеллект арқылы көңіл-күйді талдау мен чатботтарды біріктіру механизмін қолданатын «шабуыл моделі» анықталды. Көңіл-күйді талдауды террористер интернеттегі адамдардың мінез-құлқына негізделген одақтас немесе құрбанды (жертва) таңдау үшін пайдаланады. Құрбандарды іздеу кезінде олар жасанды интеллектке жас, жыныс, отбасылық жағдай, табыс деңгейі және саяси көзқарастар сияқты параметрлерді енгізеді. Құрбанның кәсібін білу оның төлем қабілеттілігі туралы және егер ол тікелей шабуыл жасаса, оған қарсы тұра алатындығы туралы ақпарат береді. Ықтимал құрбанның қозғалысы туралы ақпарат (әлеуметтік желілердегі ақпарат негізінде) құрбанға ғана емес, сонымен бірге назардағы адаммен қарым-қатынасатын адамдарға, ең алдымен саяси іс-шараларда (егер бұл адамдар құрбанмен әлеуметтік медиа арқылы байланыспаса) қауіп төндіруі мүмкін. Егер террористер назарындағы адам қандай саяси іс-шараларға қатысып жатқанын білсе, олар жалған іс-шараға қатысуға шақыру үшін өзін құрбанның саяси көзқарасымен ортақ адам ретінде көрсететін чатботты қолдана алады. Құрбанның эмоционалды байланысы туралы ақпаратты террористер чатботтың өзін құру үшін материал ретінде пайдаланады. Осылайша, террористер құрбанды ұрлануы немесе өлтірілуі мүмкін белгілі бір жерге алдап әкелуі мүмкін.

Егер террористер EMBERS сияқты болжамды талдау механизмін иемденсе, олар әлеуметтік толқулар кезінде ауқымды Террористік актілерді ұйымдастыра алады. Мысалы, террористер діндарлығы жоғары елдерде болжамды наразылықтар кезінде жаппай кісі өлтіруді қолдан жасауы мүмкін. Олар сенушілер тұратын немесе олар баратын аудандарда мүмкіндігінше көп адамды өлтіруге тырысуы мүмкін. Бұл аймақтағы әлеуметтік және психологиялық шиеленістің дәрежесі террористік актілердің объектілерін таңдаудың қосымша критерийі болуы мүмкін. Кісі өлтіруден кейін (немесе тіпті жасанды интеллект қолданылса, кісі өлтіру кезінде) террористік ұйым интернет-боттардың көмегімен екі мүмкін түрдегі хабарламаларды жібере алады:
1. Террористердің өздері (ол кезде олар өздерін ұлт-азаттық қозғалысының мүшелері деп атайды), үкіметті кісі өлтірді деп айыптайды және азаматтарды өз діндерін ғана емес, сонымен бірге өз өмірі мен денсаулығын, сондай-ақ отбасыларының денсаулығын қорғауға шақырады.
2. Мемлекеттік органдардың, ірі дәстүрлі діни ұйымдардың, террористтік ұйымның басқа да қарсыластарының атынан кісі өлтіру жауапкершілігін өз мойнына алулары туралы жалған хабарламалары.

Бұл хабарламалар кісі өлтіруді заңды үкіметке немесе террористер қорлаған дінге қарсы көтеріліс жасағандар үшін әділетті кек ретінде көрсетуі мүмкін, бұл қақтығыстың діни аспектісіне баса назар аударылады. Эффект deepfake технологиясымен күшейтілуі мүмкін, бұл кез келген саясаткермен немесе діни көшбасшымен бірдеңе айтып, жалған

[4] Nytimes.com. (2022, June 25). Retrieved October 24, 2022 [Electronic resource] – Access mode: https://www.nytimes.com/2022/06/25/technology/china-surveillance-police.html (Access data: 24.07.2023).

адамдар жасауға мүмкіндік береді. Конфессияаралық шиеленіс күшейіп келе жатқан елдерде (әсіресе элиталар мен халықтың едәуір бөлігі әртүрлі конфессияларға жататын елдерде) және әсіресе ұзаққа созылған азаматтық қақтығыс қаупіне тап болған елдерде мұндай хабарламалар халықтың едәуір бөлігін террористік ұйымдардың жағына шығаруы мүмкін. Хабарламалардың екі түрі де кісі өлтіруге кінәні басқа мемлекеттің үкіметіне (террористік ұйымның қарсыласы) жүктей алады, бұл осы мемлекеттің одақтасы болып табылатын кейбір елдерде әлеуметтік толқулар тудыруы мүмкін және осы елдерден жаңа жалдаушылардың террористік топтарға келуі мүмкін.

*Алдын алу шараларына қатысты ұсыныстар.* Осылайша, жасанды интеллект механизмдері қысқа уақыт ішінде көптеген ықтимал құрбандарды таба алады (оны талдаушы адамдар тобы жасай алмайды) және басымдықты (приоритетный) құрбан-дардың тізімін жасай алады. Бірқатар синхрондалған кісі өлтірулерден кейін террористік ұйым террористік актілер үшін жауапкершілікті өз мойнына алып, хабарламалар жібере алады, бұл азаматтардың өз үкіметіне деген сеніміне нұқсан келтіруі және жаппай әлеуметтік толқулар мен жаңа жалдаушыларды террористік әрекетке белсенді түрде тартуы мүмкін. Басқа сценарийде террористер одақтас үкіметтердің атынан (мысалы, терроризмге қарсы коалиция шеңберінде) әр елде белгілі бір санаттағы адамдарды өлтіргені үшін жауаптылығы туралы жалған ақпаратты таратуы мүмкін. Ол дағдарысқа саналы түрде жауап беруге уақыттың жетіспеушілігін ескере отырып, ел басшыларының ойланбаған шешімдеріне әкелуі мүмкін, соның ішінде әскери күш қолдану туралы шешім де бар. Террористер бұл үшін терең жалған адамдарды қолдана алады.

Жасанды интеллект арқылы ықтимал қауіпті аймақтардағы адамдардың қозғалысын немесе олардың күнделікті маршруттардан атипті ауытқуларын бақылауды бағалау да шабуылдың алдын алуға көмектеседі. Алайда, бұл мониторинг адамдарға қауіп төнбеу шарты бұзылмаса, адамдардың демократиялық құқықтары мен жеке бостандықтарына нұқсан келтірмеу үшін белсенді болмауы керек.

Жасанды интеллекттің бар мүмкіндіктерін талдау түбегейлі жаңа қауіптерді анықтауға мүмкіндік береді. Адамзат, оның ішінде жоғары деңгейдегі стратегиялық шешімдер қабылдайтын топ-менеджерлер, енді тез өзгеретін экономикалық, саяси және әлеуметтік реалияларды түсінетін күйде емес. Технология адамдардың ілгерілеуі үшін тым тез дамып келеді және технологиялық прогресс барлық әлеуметтік процестерге әсер етеді. Зерттеушілер адамның санасы объективті реалиялардан артта қалғанын мойындайды. Сондықтан қоғамды ықтимал қауіптер туралы ескертетін, оларды азайту жолдарын ұсынатын және қажет болған жағдайда адам шешімдерін адамдардың игілігі үшін реттей алатын талдау механизмдерін әзірлеу үшін озық технологияларды – үлкен деректерді талдау, жасанды интеллект, машиналық оқыту, жаңа коммуникациялық мүмкіндіктер және т.б. жүйелі түрде пайдалану өте маңызды. Сонымен қатар жасанды интеллект қоғамдық санаға әсер етудің «дәстүрлі» механизмдерін қалай күшейте алатынын түсіну үшін гуманитарлық білімнің әртүрлі салаларындағы зерттеу нәтижелерін талдау қажет[5].

*Қорытынды.* Халықаралық тәжірибені талдау жасанды интеллектті қолдану терроризмді болжау мен оған қарсы күресте ақталатынын көрсетеді.

Сонымен қатар жасанды интеллектті кең көлемде енгізу кезінде, әсіресе бетті тану немесе қоғамдық орындарда бақылау сияқты сезімтал қосымшалармен бірқатар проблемалар туындайды. Терроризмге қарсы күресте жасанды интеллектті пайдалануды қиындататын басым келіспеушіліктер технологияның Конституциялық, этикалық және заңды түрде енгізілуін қамтамасыз

[5] Artificial Intelligence and New Threats to International Psychological Security. (n.d.) / Russia in Global Affairs. Retrieved October 31, 2022 [Electronic resource] – Access mode: https://eng.globalaffairs.ru/articles/artificial-intelligence-and-new-threats-to-international-psychological-security/ (Access data: 24.07.2023).

ету қажеттілігіне бағытталған. Қоғамдық орындарда орнатылған жасанды интеллект басқаратын бақылау камералары адам құқықтарының бұзылуымен байланысты, өйткені жасанды интеллект технологиялары қаруды заңды түрде ұстап жүрген адам екенін анықтай алмайды[6].

Осыған байланысты туындайтын екінші аспект терроризм саласындағы жұмыс тәжірибесінде жасанды интеллекттің соңғы технологияларын қолдану қазіргі уақытта белгілі бір шектеулерге ие, өйткені терроризмнің қатысуын немесе қаупін болжау үшін жасанды интеллектті қолданудың нақты ережелері ішінара немесе мүлдем жоқ. Шектеулер бар жерде олар көбінесе деректердің қалай пайдаланылатындығына емес, деректерге қол жеткізуге бағытталған. Бұл шектеулер тиімді модельдер жасауға және пропорционалдылық шарттарын сақтауға және адамдарға қатысты кемсітушілікке жол бермеуге мүмкіндік бермейді.

Деректерге кеңірек қол жеткізу әрқашан адам құқықтары үшін зиянды екенін және деректерді талдауды орталықтандыру оның мәні бойынша зиянды екенін ескерген жөн.

Сонымен қатар терроризмге қарсы күресте жасанды интеллектті қолдану кезіндегі дилеммалар жалпы барлау саласындағы үлкен деректер технологиясын қолдану және терроризмге қарсы күрес адамдарды басқаруға байланысты HUMINT-тегі кейбір дәстүрлі дилеммаларды бейтараптандырады (НАТО HUMINT-ті «адамдар жинаған және ұсынған ақпараттан алынған барлау категориясы» деп анықтайды) [4, 611 б.].

Жасанды интеллектті сәтті қолданудың тағы бір проблемалық аспектісі-террористік ұйымдарға террористік актілердің салдарын қоздыруды жеңілдететін геосаяси қарама-қайшылық; жаһандық экономикалық дағдарыстардан туындаған әлеуметтік тұрақсыздық; саяси партиялар мен мемлекеттік институттарға деген сенімнің жоғалуы; озық технологияларды, әсіресе жасанды интеллект пен роботтандыруды енгізу арқылы жұмыс орындарының жоғалуынан туындаған қорқыныш пен сенімсіздіктің артуы.

Жасанды интеллект әсерінен дағдарыстың тез жеделдеуі және таралуы (бірнеше елдердегі террористік актілерді бұрын-соңды болмаған құрбандармен үндестіру) мемлекеттік органдарды негізделген шешімдер қабылдауға қажетті уақыттан айырады және оларды халықаралық аренада ойға салынбаған эмоционалды қадамдарға итермелейді[7].

Озық технологиялардың құнын төмендету оларды бір операцияның бір бөлігі ретінде біріктіруге мүмкіндік береді, бұл жауап немесе алдын алу шараларын қабылдауды қиындататын қосымша фактор болуы мүмкін. Мысалы, террористер келесі сценарийлерде дрондарды қару ретінде қолдана алады, бұл мұндай құрылғыларды бақылау және бейтараптандыру үшін жасанды интеллектті қолдануды талап етеді.

*Терроризмге қарсы ішкі күресте жасанды интеллектті потенциалды пайдалану бойынша ұсыныстар:*

- ішкі терроризммен күресу үшін жасанды интеллектті қолдану белгілі бір қоғамдық орындарда тұлғаны тану технологиясын енгізу болып табылады;
- жеке өмірге қол сұғылмаушылық туралы заңдардың сақталуын қамтамасыз ету және жаппай қадағалаудың алдын алу;
- қауіпсіздік органдарымен MUAI жайлы үкімет, саясаткерлер, қоғамдық белсенділер, жалпы жұртшылықты ақпараттандыру;
- жасанды интеллект көмегімен қоғамдық іс-шараларды қадағалайтын арнайы орталықтар құру;
- іс-шараның виртуалды сертификатының бар-жоғын тексеру мүмкіндігімен азамат олар туралы ақпараттың өзектілігін растау мақсатында жария іс-шараларды сертификаттау;
- олардың пайда болу факторларының кең ауқымын ескере отырып, жасанды интеллект арқылы саяси және дінаралық қақтығыстардың алдын алу және болжау үшін мемлекеттік және ұлттық агенттіктердің болжамды талдау механизмдерін кеңінен

[6] The AI Revolution and Its Implications on Domestic Counterterrorism / Middlebury Institute of International Studies at Monterey, 2021 [Electronic resource] – Access mode: https://www.middlebury.edu/institute/academics/centers-initiatives/ctec/ctec-publications/ai-revolution-and-its-implications-domestic (Access data: 24.07.2023).

[7] Artificial Intelligence and New Threats to International Psychological Security. (n.d.) / Russia in Global Affairs. Retrieved October 31, 2022 [Electronic resource] – Access mode: https://eng.globalaffairs.ru/articles/artificial-intelligence-and-new-threats-to-international-psychological-security/ (Access data: 24.07.2023).

қолдануы.


**Пайдаланылған әдебиеттер тізімі:**

1. Бахтеев, Д.В. Искусственный интеллект: этико-правовые основы. – 2021. – 179 с.
2. De Dominicis, L. Video-based fusion of multiple detectors to counter terrorism // Counterterrorism, Crime Fighting, Forensics, and Surveillance Technologies V. / L. De Dominicis, et al. – SPIE, 2021. – T. 11869. – Pp. 75-85.
3. Brundage, M. The malicious use of artificial intelligence: Forecasting, prevention, and mitigation / M. Brundage, et al. – arXiv preprint arXiv:1802.07228. – 2018. – 101 p.
4. Ganor, B. Artificial or Human: A New Era of Counterterrorism Intelligence? / B. Ganor / Studies in Conflict & Terrorism. – 2021. – №7(44). – Pp. 605-624. – DOI: 10.1080/1057610X.2019.1568815.

**References:**

1. Bahteev, D.V. Iskusstvennyj intellekt: jetiko-pravovye osnovy. – 2021. – 179 s.
2. De Dominicis, L. Video-based fusion of multiple detectors to counter terrorism // Counterterrorism, Crime Fighting, Forensics, and Surveillance Technologies V. / L. De Dominicis, et al. – SPIE, 2021. – T. 11869. – Pp. 75-85.
3. Brundage, M. The malicious use of artificial intelligence: Forecasting, prevention, and mitigation / M. Brundage, et al. – arXiv preprint arXiv:1802.07228. – 2018. – 101 p.
4. Ganor, B. Artificial or Human: A New Era of Counterterrorism Intelligence? / B. Ganor / Studies in Conflict & Terrorism. – 2021. – №7(44). – Pp. 605-624. – DOI: 10.1080/1057610X.2019.1568815.


**АВТОРЛАР ТУРАЛЫ МӘЛІМЕТТЕР / СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS**


**Мұхтар Бейбітұлы Садықов** – Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясының докторанты, заң ғылымдарының магистрі, мемлекеттік басқару магистрі, e-mail: mukhtar.sadykov@gmail.com.

**Садыков Мухтар Бейбутович** – докторант Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, магистр юридических наук, магистр государственного управления, e-mail: mukhtar.sadykov@gmail.com.

**Sadykov Mukhtar Beybutovich** – doctoral student of the Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, Master of Law, Master of Public Administration, e-mail: mukhtar.sadykov@gmail.com.

**Ане Арзиевна Тыныш баева** – Қазақстан Республикасы Президентінің жанындағы Мемлекеттік басқару академиясының профессоры, әлеуметтану ғылымдарының докторы, профессор, e-mail: a.tynyshbayeva@apa.kz.

**Тынышбаева Ане Арзиевна** – профессор Академии государственного управления при Президенте Республики Казахстан, доктор социологических наук, профессор, e-mail: a.tynyshbayeva@apa.kz.

**Tynyshbayeva Ane Arzievna** – Professor of the Academy of Public Administration under the President of the Republic of Kazakhstan, Doctor of Sociological Sciences, Professor, e-mail: a.tynyshbayeva@apa.kz.