



ХҒТАР 11.01.11
Ғылыми мақала

<https://doi.org/10.32523/2616-6887-2025-150-1-105-119>

Заманауи биотерроризм мәселесін шешуде киберқауіпсіздік шараларын қолдану тиімділігі

М.К. Дюсембекова^{ib}, Д.С. Примбетов^{ib}, А. Расилхан^{ib}

Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан

(E-mail: maira.enu@mail.ru, dr.dauren@mail.ru, rassylkhan.assel@gmail.com)

Аңдатпа. Қазіргі дәуірде биологиялық қауіпсіздіктің сенімді шараларын енгізу қажеттілігі артып келеді, бұл алдыңғы кезеңдердің талаптарынан асып түседі. Ұлттық және халықаралық ауқымда биоқауіпсіздік биологиялық қауіптерді азайту үшін жедел әрекет ету механизмдерінің тиімділігіне және халықтың әл-ауқаты мен мүдделерін қорғауға және ілгерілетуге ықпал ететін басқа факторларға байланысты.

Бұл елеулі жұқпалы аурулардың алдын алуға және емдеуге, биологиялық соғыс агенттерінен қорғауға және биотерроризм актілерінің алдын алуға бағытталған шараларды қамтиды. Сонымен қатар, ол биологиялық ресурстардың, оның ішінде зертханалардың қауіпсіздігін қамтамасыз етеді және қауіпті организмдердің адам популяциясы мен қоршаған ортаға енуіне жол бермейді.

Биотеррорлық қауіптерді жоюдың маңызды аспектісі биоқауіпсіздікке қатысты маңызды ақпараттық жүйелерді нығайту үшін киберқауіпсіздіктің озық әдістерін пайдалану болып табылады. Бұл шаралар осалдықтарды анықтауға және құпия деректерге рұқсатсыз қол жеткізуді болдырмауға көмектеседі, осылайша ықтимал қауіптерге жалпы төзімділікті арттырады.

Болашақтағы оқиғалардың алдын алу және жекелеген мемлекеттердің қауіпсіздік мүмкіндіктерін арттыру үшін халықаралық ынтымақтастықты нығайту өте маңызды. Бұған дәстүрлі биоқауіпсіздік шараларын озық киберқауіпсіздік технологияларымен біріктіру арқылы қол жеткізуге болады. Мұндай тәсіл маңызды ақпаратты қорғауды қамтамасыз етуге және ықтимал шабуылдардың алдын алуға көмектеседі, осылайша әлемдік қоғамдастықтың жалпы қауіпсіздігіне ықпал етеді.

Түйін сөздер: биотерроризм, биологиялық қару, ұлттық қауіпсіздік, халықаралық ынтымақтастық, биологиялық соғыс, төтенше жағдай, киберқауіпсіздік шаралары.

Түсті: 05.06.2024; Мақұлданды: 22.01.2025; Онлайн қолжетімді: 30.03.2025

Кіріспе

Қазіргі уақытта биологиялық қорғау мүмкіндіктеріне жаңа талаптар қойылуда, олар төтенше жағдайда жұмыс істейтін персоналдың, бірінші кезекте қажетті құралдардың, мамандандырылған дәрілік препараттар мен вакциналардың, емдеуге арналған тиісті жабдықтардың, сондай-ақ мониторинг және ерте хабарлау жүйелерінің болуын қамтиды. Бұдан басқа, биологиялық шабуылдан зардап шеккен жерлерді кәдеге жарату, қалпына келтіру және қайта құру мәселелеріне, сондай-ақ биоқауіпсіздік технологияларының құқықтық аспектілеріне ерекше назар аударылуы тиіс.

Жаһандану, цифрландыру және биотехнологияның қарқынды дамуымен қатар Халықаралық қауіпсіздік саласындағы түбегейлі өзгерістер «Қазақстан Республикасының биологиялық қауіпсіздігі туралы» Қазақстан Республикасының 2022 жылғы 21 мамырда бекітілген Заңды әзірлеудің алғышарты болды. Бұл заң жұқпалы аурулармен, биотерроризммен және биоқорғалу мен биоқауіпсіздік саласындағы басқа да заманауи қауіптермен байланысты жаңа тәуекелдер мен проблемалардың пайда болуына жауап болуы тиіс. Алайда қарқынды заманауи зерттеулердің дамуынан пайда болатын, биоқауіпсіздікке әсер ететін ықтималдықтардың барлығын қамту мүмкін емес.

Биологиялық қауіпсіздікті қамтамасыз ету жүйелі тәсілді және мұқият ұйымдастыруды талап етеді, бұл ұлттық деңгейде мамандандырылған заңнамалық актілерде бекітілген шаралардың кең спектрін іске асыруды, сондай-ақ оларды биоқауіпсіздік мәселелері жөніндегі халықаралық конвенциялар шеңберінде үйлестіруді білдіреді.

Заманауи цифрлық және басқа да серпінді технологияларды енгізу және белсенді қолдану «Төртінші өнеркәсіптік революция» немесе жаңа әлеуметтік-экономикалық, саяси және құқықтық шындықты біртіндеп қалыптастыратын цифрлық революцияның пайда болуына әкелді. IT-технологиялар мен интернеттің кең мүмкіндіктері бірегей технологиялық және әлеуметтік-экономикалық орталығын қалыптастырады [1].

Нәтижесінде, оларды пайдалануға байланысты туындайтын тәуекелдер мен қатерлерді азайтуға бағытталған жаңа технологияларды реттеу саласындағы жалпы теориялық және практикалық зерттеулерге ғылыми қызығушылық артып келеді.

Үлкен экономикалық және әскери әлеуеті бар ең қарқынды дамып келе жатқан жоғары технологиялық салалардың бірі бүгінде биотехнология саласы (Biotech) болып саналады. XXI ғасыр көбінесе биомедициналық ғасыр деп аталатыны кездейсоқ емес. Сандық технологиялардың арқасында көптеген ауруларды диагностикалау, емдеу, алдын алу және оңалту әдістерін түбегейлі өзгертуге қабілетті генетикалық және басқа технологиялар қарқынды дамып келеді [2].

Алайда, сол технологиялар қоғам мен мемлекеттің қауіпсіздігіне елеулі қауіп төндіріп, айтарлықтай зиян келтіруі мүмкін. Мысалы, АҚШ барлау қауымдастығы геномды өңдеу технологиясын «жаппай қырып-жою қарулары» тізіміне енгізді. Келесі 30 жыл ішінде ғалымдар синтетикалық биология токсиндерді анықтауға, өнеркәсіптік қалдықтардан биоотын өндіруге және адаммен симбиозда жұмыс істейтін дәрілерді жасауға қабілетті инженерлік организмдерді қамтамасыз етуге уәде береді. Сонымен қатар, синтетикалық биология табиғи экожүйелерді бұзуға қабілетті жасанды биологиялық қарулар мен

инвазивті синтетикалық организмдерді жасау мүмкіндігін қоса алғанда, елеулі тәуекелдерге ие [3].

Зерттеу әдістері

Бұл мақалада авторлар зерттеудің сапалық және сандық әдістерін біріктіретін кешенді тәсілді қолданады. Негізгі қолданылған әдістер:

1. *Әдебиеттер мен құжаттарды талдау.* Киберқауіпсіздік және биотерроризм саласындағы ғылыми жарияланымдар, нормативтік-құқықтық актілер және халықаралық стандарттар зерттеліп, қолданыстағы тәсілдер мен проблемаларды анықтау мүмкіндіктерін зерттеу.

2. *Жүйелік және салыстырмалы талдау.* Биотеррорлық актілердің ықтимал әсері тұрғысынан ақпараттық жүйелердің қауіптері мен осалдықтары бағаланып, әртүрлі елдерде қолданылатын әртүрлі киберқорғау шаралары салыстырылды.

3. *Сценарийлерді модельдеу және болжау.* Қорғаныс шараларының тиімділігін бағалау және қауіп-қатерге қарсы басымдықтарды анықтау үшін кибершабуыл модельдері қарастырылып, оқиғалардың ықтимал даму сценарийлерін талдау.

Мұндай көп қырлы тәсіл биотерроризмнің қазіргі заманғы қауіп-қатерлерімен күресу контекстінде киберқауіпсіздік шараларын қолданудың тиімділігін жан-жақты бағалауға және қорғаныс стратегияларын одан әрі жетілдіру бойынша ұсыныстар қалыптастыруға мүмкіндік береді.

Нәтижелер мен талқылаулар

2019 жылдың аяғында Қытайда басталған COVID-19 коронавирустық пандемиясы адамзаттың биологиялық қауіптерге қарсы тұруға дайындығы үшін үлкен сынақ болды.

Дүниежүзілік денсаулық сақтау ұйымы (ДДҰ) «биоқорғалу» (Biosafety) мен «биоқауіпсіздік» (Biosecurity) ұғымдарын ажырата отырып, бірінші ұғым патогендер мен токсиндердің кездейсоқ әсерінен сақтандыру мақсатында қолданылатын принциптерді, технологиялар мен әдістерді пайдалануды білдіреді. Бұл шаралар медико-биологиялық зертханалар қызметкерлері мен басқа да тұлғалардың жабдықтың ақаулығы немесе жұмысты ұйымдастырудағы қателіктер – мысалы, ауа өңдеу немесе қалдықтарды дезинфекциялау кезінде – себеп болатын жұқпалы аурулар қаупін азайтуға бағытталған.

Ал екінші ұғым: биоқауіпсіздік – патогендер мен токсиндердің жоғалуын, ұрлануын, дұрыс пайдаланылмауын немесе сыртқа шығуын болдырмауға арналған институционалдық және жеке шаралар кешені болып табылады. Мұнда нысандарға қол жеткізуді бақылау, материалдар мен мәліметтерді дұрыс сақтау, сондай-ақ оларды жасау әдістері туралы ақпараттың таралуын шектеу маңызды рөл атқарады. Бұл қауіптер үлгілердің араласуы, көп уақыт бұрын жойылған вирустардың «қайта тірілуі» немесе вакцинасы мен тиімді дәрі-дәрмектері жоқ патогендердің жасалуымен байланысты.

Сонымен қатар, биологиялық қару-жарақтың қолданылуы мен биотерроризммен байланысты қауіп-қатерлерге ерекше назар аударылады. Мұндай жағдайларда

жоғары патогенді бактериялар, вирустар мен токсиндер әскери немесе террористік операцияларда адамдар, жануарлар немесе өсімдіктер арасында жұқпалы аурулар, аурулар мен өлім-жітім тудыру мақсатында пайдаланылады, бұл әлеуметтік тұрақтылық пен ұлттық қауіпсіздікке теріс әсер етуі мүмкін. Биологиялық қару-жарақтың байқалуы қиын, әртүрлілігі мен әсер ету жылдамдығы оның ерте диагностикасы мен медициналық анықтамасын жүзеге асыруды аса қиындатып, оның қолданылу нәтижелері патоген түріне, шабуыл тәсіліне және қоршаған ортаның басқа да факторларына байланысты айтарлықтай өзгеруі ықтимал.

1975 жылғы бактериялық (биологиялық) және токсиндік қаруды жасау, өндіру және жинақтауға тыйым салатын халықаралық Конвенция тиімді тексеру шараларын қарастырмайды және қорғаныс мақсатында биологиялық қаруды жасауды шектемейді. Дегенмен, Конвенцияға қатысушы мемлекеттер бірінші – профилактикалық немесе қорғаныс мақсаттарына арналмаған микробиологиялық немесе басқа да биологиялық агенттер мен токсиндерді жасау, өндіру, жинақтау немесе иемденуден, екінші – әскери қақтығыстар мен жаулас әрекеттер кезінде олардың қолданылуына мүмкіндік беретін қару-жарақ, жабдық немесе жеткізу құралдарын сатып алудан бас тартуға міндетті. Сонымен қатар, Конвенцияның қосымша хаттамалары медико-биологиялық зерттеулер жүргізу үшін рұқсат алуды және пациенттердің хабардар болуы туралы келісім алуды талап етеді.

Сонымен қатар, биотерроризмге қарсы күресте айтарлықтай үлес қосқан 2005 жылғы ЮНЕСКО-ның «Биоэтика және адам құқықтары туралы» жалпы декларациясымен биоалуантүрлілікті жалпы адамзат міндеті ретінде сақтау міндеттемесін бекітілген және мемлекеттерді органдардың, үлгілердің, генетикалық ресурстар мен материалдардың заңсыз айналымына қарсы, сонымен бірге биотерроризмге қарсы күресу шараларын қабылдауға шақырады.

Биологиялық қаруды қолдану фактісі бүкіл әлемде кең көлемде наразылық толқынын туғызды, соның нәтижесінде, 1925 жылдың 17 маусымында Женевада "Соғыста тұншықтырғыш, улағыш және сол сияқты басқа газдар мен бактерологиялық заттарды қолдауға тыйым салу хаттамасына" қол қойылды [4] және 1972 жылы қабылданып, 1975 жылы күшіне еңген Біріккен ұлттар ұйымының Конвенциясы (қазіргі уақытта 165 мемлекет ратификациялады) қабылданды [5]. Дегенмен, бұл құжаттар көптеген елдерде биологиялық зерттеулерді әскери мақсатта қолдану үрдісін тоқтата алмады.

Тарихта, әсіресе соңғы бірнеше онжылдықта өлімге әкелетін жаппай қырып жоятын қарудың бұл түрі бірнеше рет қолданылған. Атап айтқанда, Италия оны Ливия мен Эритреяда, Франция Солтүстік Африкада, мысалы, Тунисте, Жапония Қытайдың Манжуриясында, Египет Йеменде, АҚШ Вьетнамда, Үндістанда және Қытайда, КСРО Ауғанстанда, Ирактың Иранға қолдануы және тағы басқалары. Мұндай қаруды қолданудың соңғы фактілері 2014 жылдың соңында Ирактың Анбар провинциясында химиялық қаруды қолданған «Ислам мемлекеті» бөлімшелерінің шабуылы болды. Дәл осы жылдың 22 қазанында күрдтердің Кобани қаласында осыған ұқсас шабуыл болды.

2018 жылы канадалық вирусолог Дэвид Эванс қарапайым «биохакердің» «тұрмыстық жағдайда» қоғамға қауіпті вирусты жасай алатындығын дәлелдеп берді. Соңғы екі факт,

биологиялық қаруды тек мемлекеттік деңгейдегі қолдаумен үлкен қаржыландырудың нәтижесінде ғана жасап шығаруға болады деген көзқарастың қате екендігінің дәлелі бола алады [6]. Ұзақ уақыт бойы лаңкестердің биологиялық қаруға ие болу мүмкіндігі өз деңгейінде қарастырылмай келді. Өйткені мұндай қару жасау жабық ғылыми-медициналық немесе әскери зертханаларды, арнайы білімді кадрларды қажет етеді. Кейбір террористік топтар мұндай шығындарды көтере алмағандықтан лаңкестіктің «дәстүрлі», «арзан» әдістерін қолдануға (жарылыстар, өртеу, кепілге алу және т.б.) мәжбүр болды. Бірақ қазіргі ғылым мен техниканың қол жетімділігінің арқасында олардың да әдіс-тәсілдері жетіліп келеді. Сондықтан, қазіргі уақытта мемлекеттер мен халықаралық ұйымдар қауіпсіздік шараларын қайта қарап, жаппай қырып жоятын қарудың бұл түрімен күресуде жаңа механизмдерді ойластыруы қажет.

Биологиялық терроризм медициналық, экономикалық, саяси және әскери зардаптарға әкелуі мүмкін. Медициналық зардаптарға – адамдардың жаппай аурулары, үрейлі нәтижелер, дүрбелең, қорқыныш, психоневрологиялық бұзылулар, мүгедектік, медициналық ресурстардың сарқылуы, медициналық мекемелердің жетіспеушілігі жатады [7].

Экономикалық зардаптар – ауылшаруашылық жануарларының жаппай ауруы мен өлімі, дәнді-дақылдарының жойылуы – халық үшін негізгі азық-түлік көзінің азаюы немесе жетіспеушілігі, жаппай аштық, босқындар санының көбеюі, күйреу, мемлекеттің сауда серіктесі ретінде әлемдік нарықтағы беделінің түсуі, эпидемияға қарсы карантиндік және эпидемияны жою шараларына шамадан тыс материалдық және қаржылық шығындар. Бұл өз кезегінде «домино әсерімен» экономиканың басқа да институттарының құлдырауына әкелуі мүмкін.

Саяси және әскери салдары – қажетсіз, «әлсіз» саяси көшбасшыларды жою немесе шантаж жасау, ел басшылығына сенімсіздік атмосферасын құру, саяси оппозицияның күшеюі, қарулы күштерді тікелей қақтығыссыз жасырын түрде әлсірету. Жоғарыдағы проблемаларды Елбасы Н.Назарбаевтың 2020 жылдың 8 сәуіріндегі мақаласында нақты атап өтті: «Жаһан жұртшылығын әбігерге салған пандемия жаңа бүкіл әлемде экономикалық дағдарыс туғызды. Алып кәсіпорындардың жұмысы тоқтады, көлік атаулының қозғалысы шектелді. Мұнайдың бағасы құлдырады. Ел мен ел арасындағы шекаралар жабылып, алыс-беріс тиылды. Мұның бәрі бұрын-соңды болмаған аса ауқымды рецессияға әкеліп соқтырып, жұмыссыздықты көбейтіп отыр» [8].

Мұндай қиын қыстауда мемлекеттің қауіпсіздік потенциалы, экономикалық, әскери қоры мықты болуы керек. «Бізде осындай қиындық туғанда ешкімге алақан жаймау үшін, ұрпақ қамы, ел болашағы үшін жинақталған Ұлттық қор мен алтын-валюта қорында 90 миллиард АҚШ доллары бар. Ретімен, үнемді пайдаланар болсақ, ол бүгін басымызға түскен тағдыр мен тарих сынынан еңсемізді тік ұстап өтуімізге мол мүмкіндік береді» [8]. Кейбір елдерде мұндай қорлардың болмауы терең саяси-экономикалық дағдарыстарға әкеліп жатқанын көріп отырмыз.

Биологиялық қаруды іс жүзінде қолданылған кезде (инкубация кезеңінің ұзақтығына байланысты) анықталмайды, сонымен қатар зардап шеккендердің өздері инфекция анықталғанға дейін ауруды таратушы болады. Біз бұл жағдайды Қытайдың Ухань

провинциясынан басталған коронавирус инфекциясынан (COVID-19) анық байқай аламыз. Оның шығу ошағын, тарату агенттерін тек алғашқы адам өлімі болғанға дейін ешкім оның вирус екенін анықтамады және аурудың инкубациялық кезеңінде вирус әлемнің бірнеше мемлекетіне тарап үлгерді. Бұл фактінің өзі қазіргі адамдар арасындағы коммуникация деңгейінің жоғарылығы мен жаһандану дәуірінде биологиялық қарудың адамзат үшін өте қауіпті екендігін айқындап берді.

Террористердің диверсияны қолдану әдістері (әсіресе тамақ өнеркәсібі кәсіпорындарында, сумен қамтамасыз ету және т.б.) террористік акт фактісін жасыруға мүмкіндік береді – туындаған аурулар мен уланулар технологияны дұрыс пайдаланбағандыққа, кәсіпорындардағы аварияларға және т.б. жағдайларға байланыстыруы мүмкін. Сонымен бірге, биологиялық қаруды нысанаға жеткізу сатысында және қолдану барысында табу оңай емес, тіпті, мүмкін емес. Ұзақ уақыт қауіпсіздік органдары террористік шабуыл болғанын байқамауы да мүмкін.

Қорқыныштысы, осы әдіспен адам (террорист) қауіпті ауруды әдейі жұқтыруы мүмкін. Аурудың жасырын ағымы кезінде ол басқа елге, қалаға көшіп, мүмкіндігінше көп адамдармен байланыс орнатуға тырысады: әуежайда немесе теміржол станциясында, қоғамдық көліктерде (әсіресе адамдар көп шоғырланатын кешкі уақытта), азық-түлік дүкендерінде немесе базарларда, азық-түлік өткізу пункттерінде, адам көп шоғырланатын іс-шараларда.

Сонымен бірге, биологиялық қаруды қолдану террористерге қажетті халықтың әлеуметтік-психологиялық жағдайына қатты әсер етеді. Адамдар арасында әр түрлі фобиялар дамып, психозға әкелуі мүмкін. Азаматтар хаттар алудан, қоғамдық көлікті пайдаланудан, көптеген азық-түлік немесе өнеркәсіптік тауарларын қолданудан үрейленіп, бас тартуы мүмкін. Және бұл фобиялар террористік актілердің басқа түрлеріне қарағанда анағұрлым тұрақты және кең масштабта болады. Себебі жасырын әрекет ету кезеңінің болуы (инкубациялық кезең) және қауіпті объектіні немесе адамды тану мүмкін еместігі әсер етеді. Сонымен бірге, кез-келген адамды потенциалды инфекцияны таратушысы ретінде қарағандықтан, зардап шеккен адамдарға психологиялық көмек беру іс жүзінде мүмкін емес. Мұндай жағдайды қазіргі коронавирус инфекциясынан зардап шеккендерден байқай аламыз. Мұның бәрі қоғамда шиеленіс тудырады. Мемлекетке, арнайы қызмет органдарына, аурудың көптеген өлімге әкелу нәтижесінде – ресми медицинаға деген сенімсіздік тудырады.

2019-2020 жылдардағы жағдайдың (коронавирус инфекциясына байланысты төтенше жағдайдың еңгізілуі) қайталанбауы үшін және биотерроризмнің алдын алу мақсатында халықаралық қауымдастық келешекте қажетті құжаттар қабылдап, оны нақты әрекеттермен бекітуі керек. Әрине Қазақстан Республикасы бұл мақсатта көптеген іс-шаралар атқарып келеді. Көптеген заңдар мен нормативтік актілер қабылдап, терроризмге қарсы халықаралық актілерді ратификациялады. Алайда, биологиялық терроризмнің табиғаты мен зардап көлемін ескере отырып, бұл індетке қарсы тұрудың келесі жолдары ұсынылады:

– биологиялық терроризмге қарсы халықаралық ынтымақтастықты дамыту. Химиялық және бактериологиялық қаруға тиым салу Конвенциясының орындалуын

қатал бақылау. Өйткені Конвенцияны ратификациялаған көптеген елдер жасырын түрде зерттеулер жасауда. Оларды тексеру тетіктері мен санкцияларын қаталдандырып, хаттамаларды жетілдіру керек;

- Қазақстан Республикасының әскери күштері мен құқық қорғау органдарының оқу-жаттығу бағдарламаларында міндетті түрде биологиялық және химиялық қатерге, террористік актілерге қарсы тұру алгоритмдерін жетік меңгерту қажет;

- биологиялық терроризмнің географиясы мен себептерін зерттей отырып, статистикалық талдау жасауды ұйымдастыру;

- тұрғындарды биотерроризм орын алған жағдайда қорғану және әрекет ету тәрбімен жүйелі түрде оқытуды ұйымдастыру (Азаматтық қорғану курстары). Ондай тәжірибе біздің мемлекетімізде болған. Бұндай қауіпте нақты және уақытында пайдаланған әрекет ету алгоритмі ғана бейбіт тұрғандар арасында көп шығынға жол бермейді;

- жағдайдың әр-түрлі өрбу сценарийлерін ескере отырып, шұғыл әрекет ету үшін қажетті және қосымша ресурс көздерін дайындау (зардап шеккендердің санының тым көбеюі, эпидемия уақытының созылуы, азық-түлікпен қамтамасыз ету және т.б.);

- цифрлы қызмет етудің бірнеше платформасын қолдануға жағдай жасау. Өйткені көптеген онлайн қызмет ету платформасы жаппай қызмет алуда қуаты жетпей, кейбір базалар тіпті істен шығып кету қаупі бар.

- биологиялық қауіп төнген төтенше жағдайда биологтар, химиктер және медицина қызметкерлерін тарта отырып әрекет ету тәртібін алдын ала жоспарлау.

Шетелдік тәжірибе. Соңғы жылдары көптеген елдерде биологиялық қауіпсіздікті қамтамасыз етуге бағытталған арнайы заңдар қабылдануда немесе қайта қаралуда. Сонымен, Жаңа Зеландияда биологиялық қауіпсіздік туралы Заңның (Biosecurity Law Reform Act 2012) редакциясы жаңартылды, сонымен қатар зиянкестер мен қалаусыз микроорганизмдердің елге енуіне жол бермеуге бағытталған эксклюзивті экономикалық аймақ туралы Заң қабылданды [9].

2019 жылы Австралия 2015 жылғы биоқауіпсіздік туралы Заңның жаңа редакциясын мақұлдап, оны 1908 жылғы «Карантин туралы» Заңмен алмастырды. Бұл заң адамның биоқорғанысымен байланысты тәуекелдердің кең ауқымын басқаруды реттейді-қауіпті инфекциялармен жұқтыру қаупінен бастап жер асты суларының ластануы мен экожүйедегі төтенше жағдайларға байланысты тәуекелдерге дейін. Сонымен қатар, ол халықаралық санитарлық-эпидемиологиялық ережелер (International Health Regulations 2005), ДСҰ-ның санитарлық-фитосанитарлық шаралар туралы келісімі және биологиялық әртүрлілік туралы Конвенция (Convention on Biological Diversity 1992) [10] сияқты халықаралық міндеттемелерді орындау механизмін анықтайды.

Қытайда ұлттық биоресурстарды қорғауды қамтамасыз ететін, биотехнологияларды дамытуға ықпал ететін және ҚХР ұлттық қауіпсіздігіне қауіп төндіретін биологиялық агенттер мен технологияларды пайдалануға жол бермейтін биологиялық қауіпсіздік туралы заң жобасы қарастырылуда.

Еуропалық Одақтың биоэкономика бойынша стратегиялық құжаттары (мысалы, bioeconomy Strategy, 2018; innovating for ..., 2012) шектеулі ресурстар мен климаттың өзгеруі, Жер мен экожүйелердің деградациясы және планета халқының өсуі сияқты

жаһандық сын-қатерлер жағдайында экологиялық қауіпсіздікті ескеретін өндіріс пен тұтынудың жаңа үлгілерін табу қажеттілігін көрсетеді.

Биотехнология және биомедицина саласындағы жетекші елдердің – Ұлыбритания мен АҚШ-тың ресми ұлттық биологиялық қауіпсіздік стратегиялары ерекше назар аударуға тұрарлық. 2018 жылдың қыркүйегінде АҚШ-та елді биологиялық қауіптерден қорғау, биоинциденттердің алдын алу және олардың салдарын азайту үшін Ұлттық биологиялық қорғаныс стратегиясы (National biodefense Strategy) бекітілді. АҚШ-тың Ұлттық қауіпсіздік стратегиясымен (2018) тығыз байланысты және өткен биологиялық оқиғалардың тәжірибесіне негізделген бұл стратегия қоғамға, экономикаға және қоршаған ортаға зиян келтіретін қауіптерден қорғаудың тиімді және тұрақты механизмін құруға бағытталған [11].

Бұл стратегияларда биологиялық қауіптердің екі негізгі түрі бар. Бірінші түрі-жұқпалы аурулардың трансшекаралық таралуына байланысты табиғи қауіптер. Екінші түрі-қасақана немесе кездейсоқ оқиғалардан туындайтын қауіптер, мысалы, биологиялық қаруды қолдану немесе оны мемлекеттік және мемлекеттік емес субъектілердің таратуы, бұл ұлттық қауіпсіздікке, Халыққа, ауыл шаруашылығына және экологияға үлкен қауіп төндіреді. Сонымен қатар, көптеген елдерде биологиялық қару жасаудың құпия бағдарламалары жүргізілгені, ал кейбір террористік топтар оны сатып алуға ұмтылғаны атап өтілді. Патогендердің биоқорғаныс шаралары жиі жетіспейтін зертханаларда сақталуы, бұл күтпеген салдарға әкелуі мүмкін.

Биологиялық тәуекелдерді басқару Стратегияда орталық болып табылады, өйткені ол қауіптерді терең түсінуді және дәл бағалауды, сондай-ақ АҚШ-та немесе шетелде болған оқиғаларға қарамастан жедел әрекет етуді және алдын алу шараларын қабылдауды талап етеді. Стратегия биологиялық қауіптерді толығымен жою мүмкін емес деген қағидадан туындайды, бірақ олардың әсерін бақылауға болады және қажет. Осы стратегияның арқасында АҚШ үкіметі өзінің күш-жігерін оңтайландырады және биологиялық қауіптердің кең ауқымымен күресу үшін ішкі және сыртқы серіктестермен жұмысты үйлестіреді.

Осыған ұқсас ведомствоаралық тәсіл Ұлыбританияның 2018 жылдың тамызында жарияланған биологиялық қауіпсіздік стратегиясында да жүзеге асырылды. Бұл стратегияның мақсаты – Елді және оның ұлттық мүдделерін олардың көздері мен әсер ету объектілеріне қарамастан өзекті биологиялық қауіптерден қорғау. Ұлттық Қауіпсіздік Кеңесінің кіші комитетіне есеп беретін ведомствоаралық кеңес қауіптерді басқару тетіктерін жетілдіруге және қарсы іс-қимыл шараларын әзірлеуге ықпал ететіні атап өтілді [12].

Биотерроризмнен қорғанудағы киберқауіпсіздіктің орны. Ақпараттық технологиялар мен биотехнологиялардың қарқынды бірігуі аясында киберқауіпсіздік әдістерін қолдану жаңа мағынаға ие болды. Бұл әдістер биотерроризмнің алдын алуда әлеуетті осал тұстарды анықтап, критикалық мәліметтер мен жабдыққа рұқсатсыз кіруді болдырмауға, сондай-ақ қауіп туындаған жағдайда тиімді қарсы шараларды үйлестіруге мүмкіндік береді.

Биотерроризм қауіптері екі жақты сипатқа ие: олар биологиялық кеңістік пен киберкеңістікте де туындауы мүмкін. Мысалы, зертханалық жабдықты басқару жүйесіне

жасалған шабуыл патогенді материалдардың шығуына немесе модификациялануына әкелуі ықтимал. Сондықтан киберқауіпсіздік шаралары дәстүрлі биоқауіпсіздік әдістерімен біріктіріліп, кешенді қорғауды қамтамасыз етуі қажет. Бұл үшін ақпараттық технологиялар, биотехнологиялар, физикалық қауіпсіздік және тәуекелдерді басқару салаларындағы білімдерді біріктіретін көпсалалы тәсіл қажет.

Биотерроризмнің алдын алуда киберқауіпсіздіктің негізгі бағыттары.

1. Мониторинг және ерте анықтау: биологиялық деректер мен жабдыққа қатысты ақпараттық ағындарды бақылау алдын алу шараларының маңызды бөлігі болып табылады. Қазіргі киберқауіпсіздік жүйелері генетикалық ақпарат пен патогенді микроорганизмдерге қатысты деректер базаларына рұқсатсыз кіру әрекеттерін анықтауға мүмкіндік береді. Машиналық оқыту мен үлкен деректерді талдау әдістерін қолданып, пайдаланушылардың қалыптан тыс мінез-құлықтарын анықтап, ықтимал қауіптер туындаған кезде тез әрекет етуге мүмкіндік береді [13].

2. Критикалық инфрақұрылымды қорғау

Лабораториялық кешендер, биологиялық агенттерді синтездеу өндірістік объектілері және биологиялық материалдарды сақтау мен тасымалдау жүйелері сияқты маңызды объектілерді қорғау аса өзекті. Физикалық қауіпсіздік шаралары, бейнебақылау жүйелері, рұқсатты бақылау және деректерді шифрлеу сияқты көпдеңгейлі қорғау әдістерін қолдану ақпараттың рұқсатсыз пайдаланылуы немесе ағуына әкелетін тәуекелдерді айтарлықтай төмендетеді [14].

Бұл шаралар киберқауіпсіздік жүйелерімен біріктіріліп, шабуылдардың алдын алуға арналған біртұтас қорғаныс алаңын құруға ықпал етеді.

3. Енуді тестілеу және осалдықтарды бағалау

Пентесттерді үнемі жүргізу (ену сынағы) биологиялық инфрақұрылыммен байланысты қауіпсіздік жүйелеріндегі әлсіз жерлерді анықтауға мүмкіндік береді. Бұл сынақтар ықтимал қауіптерді анықтауға ғана емес, сонымен қатар оларды жоюдың тиімді шараларын жасауға көмектеседі. Биотехнологиялық зерттеулер жүргізілетін немесе сезімтал ақпарат сақталатын жүйелер киберқауіпсіздік жөніндегі мамандарды тарта отырып, кешенді бағалаудан өтуі тиіс [15].

4. Саясаттар мен стандарттарды әзірлеу және енгізу

Биоқауіпсіздік талаптармен қатар, киберқауіпсіздік стандарттарын да қамтитын кешенді нормативтік құжаттарды әзірлеу биотерроризмнің алдын алуда маңызды рөл атқарады. Біріккен Ұлттар Ұйымы және басқа да халықаралық ұйымдар әзірлейтін стандарттар критикалық объектілерді қорғау жүйелеріне қойылатын минималды талаптарды анықтайды. Бұл стандарттар қауіпсіздік шараларын унитаризациялауға және биотерроризммен халықаралық деңгейде күресте ынтымақтастықты жеңілдетуге ықпал етеді [16].

5. Персоналды оқыту және біліктілікті арттыру

Киберқауіпсіздік шараларының тиімділігі олардың дұрыс пайдаланылуына тікелей байланысты. Биотехнологиялық зертханалар мен критикалық инфрақұрылым объектілерінде жұмыс істейтін мамандарды киберқауіпсіздік бойынша тұрақты оқыту қажет. Бұл оқыту деректерді қорғаудың техникалық аспектілерін, сондай-ақ төтенше

жағдайларда әрекет ету дағдыларын меңгеруді қамтиды. Оқыту симуляциялары мен wargames (оқу-жаттығулары) шабуыл сценарийлерін отработкалауға және топтық әрекет ету қабілетін дамытуға мүмкіндік береді [17].

Практикалық шараларға мысалдар келтірсек:

– *Деректерді шифрлеу.* Биологиялық зерттеулерге қатысты құпия ақпаратты және патогенді үлгілерді сақтау кезінде заманауи шифрлау алгоритмдерін қолдану деректерді рұқсатсыз алуға немесе пайдалануға кедергі келтіреді.

– *Көпфакторлы аутентификация.* Көпфакторлы аутентификация (MFA) қолдану жүйелеріне кіру кезінде рұқсатсыз әрекеттердің алдын алуға және деректерге қол жеткізуді қиындатуға көмектеседі.

– *Желіні сегментациялау.* Корпоративтік желіні бірнеше оқшауланған сегменттерге бөлу кибершабуылдардың таралуын шектейді. Мысалы, зертханалық жүйелерді жалпы ақпараттық жүйеден физикалық және логикалық тұрғыдан бөлу қауіпсіздікті арттырады.

– *Мониторинг және логинг.* Қолданбалы мониторинг және логинг жүйелерін енгізу барлық кіру әрекеттерін бақылауға мүмкіндік беріп, ықтимал қауіптерді тез анықтап, жылдам әрекет етуге жағдай жасайды.

– *Қауіптер мен тәуекелдерді талдау.* Тұрақты түрде қауіптер мен тәуекелдерге талдау жүргізу қауіпсіздік шараларын жаңартуға және жаңа шабуыл түрлеріне бейімделуге мүмкіндік береді.

Қорытынды

Әрине терроризмнің бұл түрімен күресуде барлық осал жақтарды жою мүмкін емес, бірақ, біз оларды барынша азайтуымыз керек. Мұндай шабуылға барынша дайын болған мемлекет, қоғам ғана тығырықтан тез шығып, зардап салдарын тез жоя алады.

Биотеррористік шабуылдың алдын-алуда террористерге үлкен кедергі келтіретін механизмдер мен бірқатар шараларды жүзеге асыру – осы зұлымдықпен күрестің ең тиімді әдісі болып табылады. Биотеррорлық шабуылдар мәселесін уақытша деп санауға болмайды, сондықтан біз әрқашан олармен күресуге дайын болуымыз керек. Шын мәнінде, белгілі бір дағдарыстарды жоюдың басты факторы, оларды тез және тиімді шеше алу мүмкіндігіне байланысты. Тиісті органдардың нақты және кәсіби (шебер) әрекеттері ғана апат көлемінің азаюын қамтамасыз етеді. Егер билік не істеу керектігін білмесе, іс-шараларды кеш қолданса немесе қажет емес әрекеттерге барса, онда бұл әрекет кері әсер беруі мүмкін, кейбір кезде жағдай бақылаудан шығып кетуі мүмкін.

Мониторингтің, енуге тестілеудің, саясатты әзірлеудің, персоналды оқытудың және заманауи технологиялық шешімдерді енгізудің тиімді үйлесімі биологиялық агенттер мен жабдықтарға рұқсатсыз қол жеткізу тәуекелдерін айтарлықтай төмендетуге қабілетті. Биотехнологиялық процестерді цифрландырудың өсуі және синтетикалық биология мүмкіндіктерінің артуы жағдайында мұндай шаралар ұлттық және халықаралық қауіпсіздіктің қажетті элементіне айналады.

Биотеррорлық шабуылдың алдын алу кешенді тәсілді талап етеді, ол киберқауіпсіздік әдістерін дәстүрлі биоқауіпсіздік шаралармен біріктіреді. Бұл қазіргі әлемде, жаңа технологиялар ғылыми прогресске үлкен мүмкіндіктер ашатын болса да, халық денсаулығы мен мемлекеттік қауіпсіздікке жаңа қауіптер тудыратын жағдайда ерекше өзекті. Киберқауіпсіздік, биотехнология және мемлекеттік басқару салаларындағы мамандардың өзара үйлесімді жұмысы тиімді қорғаныс жүйесін құруға және жаңа шабуылдарға төтеп беруге мүмкіндік береді.

Осылайша, киберқауіпсіздік әдістерін биоқауіпсіздік жүйесіне интеграциялау биотеррорлық шабуылдық қарсы күресте маңызды элемент болып табылады. Осы шараларды қабылдау және жүзеге асыру ықтимал шабуылдарды болдырмауға, инциденттер туындаған жағдайда жылдам әрекет етіп, қалпына келтіру шараларын ұйымдастыруға мүмкіндік береді, нәтижесінде адамдардың өмірі мен денсаулығын, сондай-ақ ұлттық қауіпсіздікті қамтамасыз етуге ықпал етеді.

Қаржыландыру. Мақала Қазақстан Республикасы Ғылым және жоғары білім министрлігі Ғылым комитетінің қаржылық қолдауымен орындалды (BR24993082).

Авторлардың қосқан үлесі:

М.К. Дюсембекова – ғылыми мақаланың мақсат-міндеттерін айқындау, зерттеу материалдары мен әдіс-тәсілдерді қолдана отырып жұмыс жасау, теориялық материалдарды жинақтау және талдау жүргізу.

Д.С. Примбетов – әдебиетпен жұмыс, тілдік материалдар жинау және талдау, ғылыми мақаланы талапқа сай рәсімдеу. Теориялық материалдарды жинақтау және талдау жүргізу;

А. Расилхан – әдебиетпен жұмыс, тілдік материалдар жинау және талдау, ғылыми мақаланы талапқа сай рәсімдеу.

Әдебиеттер тізімі

1. Жаворонкова Н.Г., Агафонов В.Б. Теоретико-методологические проблемы правового обеспечения экологической, биосферной и генетической безопасности в системе национальной безопасности Российской Федерации // Lex russica. – 2019. – 1(9). – С. 96-108.

2. Сергеев Е.Д., Мохов А.А., Яворский А.Н. Пилотный (экспериментальный) правовой режим для отечественной биомедицинской науки и практики // Медицинское право. – 2019. – № 4. – С. 3–13.

3. Global Innovation Index 2017: Innovation Feeding the World. [Electronic resource]. Available at: <http://www.wipo> (Accessed: 05.06.2024).

4. Protocol for the Prohibition of the Use of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare. Geneva, 17 June 1925 [Electronic resource]. Available at: <https://treaties.un.org/pages/showdetails.aspx?objid=0800000280167ca8> (Accessed: 05.06.2024).

5. Бактериологиялық (биологиялық) және токсиндік қаруды әзірлеуге, өндіруге және жинақтауға тыйым салу және оларды жою туралы Конвенция. [Электронды ресурc]. URL: https://adilet.zan.kz/kaz/docs/P050000235_ (Қаралған күні: 05.06.2024).

6. Биохакеры могут создать биологическое оружие. [Электронный ресурс]. URL: <https://hightech.plus/2018/05/15/bioweapons> (Дата обращения: 05.06.2024).
7. Саджад Абди. Биотерроризм и способы борьбы с ним. [Электронный ресурс]. URL: <https://inosmi.ru/world/20150329/227175496.html> (Дата обращения: 05.06.2024).
8. Назарбаев Н. Бірлесе білген ел бәрін жеңеді. [Электронды ресурс]. URL: <https://qazaqstan.tv/news/125358/> (Қаралған күні: 05.06.2024).
9. Biosecurity Law Reform Act 2012. [Electronic resource]. Available at: <http://www.legislation.govt.nz/act/public/2012/0073/latest/whole.html> (Accessed: 05.06.2024).
10. Fact Sheet. Biosafety and Biosecurity. [Electronic resource]. Available at: <https://www.who.int/> (Accessed: 05.06.2024).
11. Global Innovation Index 2016: Winning with Global Innovation [Electronic resource]. Available at: http://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2016 (Accessed: 05.06.2024).
12. National biodefense strategy. [Electronic resource]. Available at: <https://www.whitehouse.gov/wp-content/> (Accessed: 05.06.2024).
13. Bioeconomy Strategy. A sustainable bioeconomy for Europe: strengthening the connection between economy, society and the environment. [Electronic resource]. Available at: https://ec.europa.eu/research/bioeconomy/pdf/ec_bioeconomy_strategy_2018.pdf (Accessed: 05.06.2024).
14. Супотницкий М.В. Живая смерть: что такое биологическое оружие // Популярная механика. - 2018. - № 1.
15. Lucas Potter, Xavier-Lewis Palmer. Human Factors in Biocybersecurity Wargames [Electronic resource]. Available at: <https://arxiv.org/abs/2005.02135> (Accessed: 05.06.2024).
16. Защита критически важных объектов инфраструктуры от террористических атак - точка зрения интерпола // Защита критически важных объектов инфраструктуры от террористических атак: Сборник передового опыта. ИДКТК и КТУ ООН. - 2018 г. - С.7
17. Информационно-аналитический обзор «Особенности угрозы биологического терроризма в современных условиях». [Электронный ресурс]. URL: <https://www.cisatc.org/147058788.pdf> (Дата обращения: 05.06.2024).

М.К. Дюсембекова, Д.С. Примбетов, А. Расилхан

Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан

Эффективность применения мер кибербезопасности при решении проблемы современного биотерроризма

Аннотация. В современную эпоху все более настоятельной становится необходимость принятия надежных мер по обеспечению биобезопасности, превосходящих требования прежних времен. Как на национальном, так и на международном уровнях биобезопасность зависит от эффективности механизмов быстрого реагирования для смягчения биологических опасностей и других факторов, которые способствуют защите и продвижению благополучия и интересов населения.

Это включает меры, направленные на предотвращение серьезных инфекционных заболеваний и борьбу с ними, защиту от боевых биологических агентов и предотвращение актов

биотерроризма. Кроме того, это обеспечивает безопасность биологических ресурсов, включая лаборатории, и предотвращает попадание опасных организмов в человеческое население и окружающую среду.

Важнейшим аспектом борьбы с биотеррористическими угрозами является использование передовых методов кибербезопасности для укрепления критически важных информационных систем, связанных с биозащищенностью. Эти меры помогают выявлять уязвимости и предотвращать несанкционированный доступ к конфиденциальным данным, тем самым повышая общую устойчивость к потенциальным угрозам.

Для предотвращения будущих инцидентов и повышения потенциала отдельных государств в области безопасности крайне важно укреплять международное сотрудничество. Этого можно достичь путем интеграции традиционных мер биозащиты с передовыми технологиями кибербезопасности. Такой подход поможет обеспечить защиту критически важной информации и предотвратить потенциальные атаки, тем самым внося вклад в общую безопасность мирового сообщества.

Ключевые слова: биотерроризм, биологическое оружие, национальная безопасность, международное сотрудничество, биологическая война, чрезвычайная ситуация, меры кибербезопасности

M.K. Dyussembekova, D.S. Primbetov, A. Rassylkhan

L.N. Gumilyov Eurasian National University, Astana, Kazakhstan

Effectiveness of the use of cybersecurity measures in solving the problem of modern bioterrorism

Abstract. In the contemporary era, there is a growing imperative for implementing robust biosafety measures, surpassing the requirements of earlier times. On both the national and international scales, biosafety is contingent upon the efficacy of swift response mechanisms to mitigate biological hazards and other factors that contribute to safeguarding and promoting the well-being and interests of the populace.

This encompasses measures aimed at preventing and managing significant infectious diseases, safeguarding against biological warfare agents, and averting acts of bioterrorism. Additionally, it ensures the security of biological resources, including laboratories, and prevents the introduction of hazardous organisms into human populations and the environment.

A crucial aspect of addressing bioterroristic threats is leveraging advanced cybersecurity techniques to fortify critical information systems pertaining to biosecurity. These measures aid in identifying vulnerabilities and preventing unauthorized access to confidential data, thereby bolstering the overall resilience against potential threats.

In order to prevent future incidents and enhance the security capabilities of individual states, it is crucial to strengthen international cooperation. This can be achieved by integrating traditional biosecurity measures with cutting-edge cybersecurity technologies. Such an approach will help ensure the protection of critical information and thwart potential attacks, thereby contributing to the overall security of the global community.

Keywords: bioterrorism, biological weapons, national security, international cooperation, biological warfare, emergency, cybersecurity measures

References

1. Zhavoronkova N.G., Agafonov V.B. Teoretiko-metodologicheskie problemy pravovogo obespecheniya ekologicheskoi, biosfernoi i geneticheskoi bezopasnosti... v sisteme natsional'noi bezopasnosti Rossiiskoi Federatsii [Theoretical and methodological problems of legal support of ecological, biospheric and genetic security... in the national security system of the Russian Federation], Lex russica, 1(9), 96-108 (2019). [in Russian]
2. Sergeev E.D., Mokhov A.A., Yavorskii A.N. Pilotnyi (eksperimental'nyi) pravovoi rezhim dlya otechestvennoi biomeditsinskoi nauki i praktiki [Pilot (experimental) legal regime for domestic biomedical science and practice], Meditsinskoe pravo [Medical law], 4, 3-13 (2019). [in Russian]
3. Global Innovation Index 2017: Innovation Feeding the World. [Electronic resource]. Available at: <http://www.wipo> (Accessed: 05.06.2024).
4. Protocol for the Prohibition of the Use of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare. Geneva, 17 June 1925 [Electronic resource]. Available at: <https://treaties.un.org/pages/showdetails.aspx?objid=0800000280167ca8> (Accessed: 05.06.2024).
5. Bakteriyalogiyalyk (biologiyalyk) zhane toksindik karudy azirleuge, ondiruge zhane zhinaktauga tiyym salu zhane olardy zhoyu turaky Konvetsiya [Convention on the Prohibition of the development, production and accumulation of bacteriological (biological) and Toxin Weapons and their destruction]. [Electronic resource]. Available at: https://adilet.zan.kz/kaz/docs/P050000235_ (Accessed: 05.06.2024). [in Kazakh]
6. Biokhakery mogyt sozdat' biologicheskoe oruzhie [Biohackers can create biological weapons]. [Electronic resource]. Available at: <https://hightech.plus/2018/05/15/bioweapons> (Accessed: 05.06.2024). [in Russian]
7. Sadzhap Abdi. Bioterrorizm i sposoby bor'by s nim [Bioterrorism and ways to combat it]. [Electronic resource]. Available at: <https://inosmi.ru/world/20150329/227175496.html> (Accessed: 05.06.2024). [in Russian]
8. Nazarbaiev N. Birlese bilgen el barin zhenedi [The country that knows together wins everything]. [Electronic resource]. Available at: <https://qazaqstan.tv/news/125358/> (Accessed: 05.06.2024). [in Kazakh]
9. Biosecurity Law Reform Act 2012. [Electronic resource]. Available at: <http://www.legislation.govt.nz/act/public/2012/0073/latest/whole.html> (Accessed: 05.06.2024).
10. Fact Sheet. Biosafety and Biosecurity. [Electronic resource]. Available at: <https://www.who.int/> (Accessed: 05.06.2024).
11. Global Innovation Index 2016: Winning with Global Innovation [Electronic resource]. Available at: http://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2016 (Accessed: 05.06.2024).
12. National biodefense strategy. [Electronic resource]. Available at: <https://www.whitehouse.gov/wp-content/> (Accessed: 05.06.2024).
13. Bioeconomy Strategy. A sustainable bioeconomy for Europe: strengthening the connection between economy, society and the environment. [Electronic resource]. Available at: https://ec.europa.eu/research/bioeconomy/pdf/ec_bioeconomy_strategy_2018.pdf (Accessed: 05.06.2024).

14. Supotnitskii M.V. Zhivaya smert': chto takoe biologicheskoe oruzhie [A living death: What is a biological weapon?], Populyarnaya mekhanika [Popular Mechanics], 1, 2018. [in Russian]
15. Lucas Potter, Xavier-Lewis Palmer. Human Factors in Biocybersecurity Wargames. [Electronic resource]. Available at: <https://arxiv.org/abs/2005.02135> (Accessed: 05.06.2024).
16. Zashchita kriticheskii vazhnykh obektov infrastruktury ot teoreticheskikh atak – tochka zreniya interpola [Protecting critical infrastructure from terrorist attacks - Interpol's point of view], Zashchita kriticheskii vazhnykh obektov infrastruktury ot teoreticheskikh atak: Sbornik peredavogo opyta [Protecting critical infrastructure from terrorist attacks: A Collection of Best Practices]. CTED and CTU of the United Nations, 2018. - P. 7. [in Russian]
17. Informatsionno-analiticheskii obzor "Osobennosti ugrozy biologicheskogo terrorizma v sovremennykh usloviyakh" [Information and analytical review "Features of the threat of biological terrorism in modern conditions"]. [Electronic resource]. Available at: <https://www.cisatc.org/147058788.pdf> (Accessed: 05.06.2024). [in Russian]

Авторлар туралы мәлімет:

Примбетов Д.С. – саясаттану кафедрасының оқытушысы, Л.Н.Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.

Дюсембекова М.К. – саясаттану кафедрасының профессоры, Л.Н.Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.

Расилхан А. – PhD докторант, Л.Н.Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.

Primbetov D.S. – Lecturer Department of Political Science, L.N.Gumilyov Eurasian National University, Astana, Kazakhstan.

Dyussembekova M.K. – Professor of the Department of Political Science, L.N.Gumilyov Eurasian National University, Astana, Kazakhstan.

Rassylkhan A. – PhD student, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan.



Copyright: © 2025 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY NC) license (<https://creativecommons.org/licenses/by-nc/4.0/>).