ҒТАХР 10.77.51
ӘОЖ 343
JEL K49

https://doi.org/10.46914/2959-4197-2026-1-1-149-158

АПАХАЕВ Н.Ж.,*[1]
з.ғ.к., профессор.
*e-mail: apahaev_nurlan@mail.ru
ORCID ID: 0000-0001-7795-2518
ЗУЛЕЕВА А.Ж.,[1]
PhD, қауымдастырылған профессор.
e-mail: ainagul.z@mail.ru
ORCID ID: 0009-0003-1049-6038
ШИДЕМОВ А.Г.,[1]
PhD, қауымдастырылған профессор.
e-mail: Sh_azem@mail.ru
ORCID ID: 0009-0001-8643-4058
[1]Q университеті,
Алматы қ., Қазақстан

ІІО ҚЫЗМЕТІНДЕ ЖАСАНДЫ ИНТЕЛЛЕКТІНІ ЕНГІЗУ АРҚЫЛЫ КИБЕРҚАУІПСІЗДІКТІ АРТТЫРУ ТЕТІКТЕРІ

Аңдатпа

Қазіргі таңда жасанды интеллект технологиялары құқық қорғау саласында түбегейлі өзгерістердің катализаторына айналып отыр. Киберқылмыстардың күрделенуі, трансшекаралық сипатқа ие болуы және цифрлық кеңістіктегі қылмыстық белсенділіктің көбеюі Ішкі істер органдарының жаңа тәсілдер мен құралдарды қолдануын талап етеді. Осы мақалада ІІО қызметіне жасанды интеллектіні енгізудің негізгі тетіктері, оның киберқауіпсіздікті қамтамасыз етудегі рөлі және практикалық іске асырудың институционалдық, құқықтық және техникалық аспектілері жан-жақты қарастырылған. Зерттеу барысында халықаралық ұйымдардың Interpol, Europol, UNICRI және OECD стратегиялық құжаттары мен ұсынымдарына, сондай-ақ Қазақстан Республикасының ұлттық цифрландыру және киберқауіпсіздік стратегияларына талдау жасалды. Зерттеу барысында ЖИ ІІО қызметіне енгізудің тиімділігін бағалау және оның киберқауіпсіздік жүйесіне ықпалын анықтау мақсатында жүйелі талдау әдісі, шетелдік және отандық тәжірибелерді салыстыру негізінде ІІО қызметінде ЖИ қолданудың ерекшеліктері мен артықшылықтары зерттелді.

Тірек сөздер: жасанды интеллект, киберқауіпсіздік, киберқылмыс, деректерді талдау, машиналық оқыту, цифрлық трансформация, құқықтық реттеу.

Кіріспе

Қазіргі заманда цифрлық технологиялардың қарқынды дамуы мен ақпараттық қоғамның қалыптасуы құқық қорғау органдарының қызметіне түбегейлі өзгерістер енгізіп отыр. Киберкеңістік адам өмірінің барлық саласына еніп, жаңа экономикалық, әлеуметтік және құқықтық қатынастарды туындатуда. Алайда, осы үдерістермен қатар киберқылмыстың түрлері мен әдістері де күрделеніп, оның ауқымы жылдан жылға кеңейіп келеді. Бұл өз кезегінде ұлттық қауіпсіздік пен қоғам тұрақтылығына елеулі қауіп төндіреді.

Киберқылмыстармен күрес – дәстүрлі тергеу және жедел-іздестіру тәсілдерімен шектелмейтін, жоғары технологиялық құралдар мен интеллектуалды талдауды қажет ететін күрделі процесс. Осы тұрғыда жасанды интеллект (әрі қарай – ЖИ) технологияларын Ішкі істер органдары (әрі қарай – ІІО) қызметіне енгізу – киберқауіпсіздікті қамтамасыз етудің жаңа кезеңіне жол ашатын өзекті бағыт. ЖИ негізінде құрылған жүйелер үлкен деректер көлемін

талдап, қауіптердің пайда болуын болжауға, күдікті әрекеттерді автоматты түрде анықтауға және тергеу процестерін оңтайландыруға мүмкіндік береді.

Соңғы жылдары әлемдік тәжірибеде құқық қорғау саласында ЖИ-дің қолданылуы айтарлықтай кеңейді. Мысалы, АҚШ, Ұлыбритания, Жапония және Сингапур секілді елдерде ІІО құрылымдары ЖИ негізінде жұмыс істейтін кибербарлау, деректерді визуалды талдау және қылмыстық мінез-құлықты болжау жүйелерін белсенді пайдалануда. Бұл технологиялар нақты уақыт режимінде деректерді өңдеу арқылы киберқылмыстық әрекеттерді ерте анықтау мен олардың алдын алуға мүмкіндік береді.

Қазақстан Республикасы да цифрлық мемлекет қалыптастыру жолында ақпараттық қауіпсіздік пен құқық қорғау жүйесін жетілдіруді стратегиялық басымдықтардың бірі ретінде айқындаған. «Цифрлық Қазақстан» мемлекеттік бағдарламасында цифрлық трансформацияны жеделдету, мемлекеттік қызметтерді автоматтандыру және ақпараттық инфрақұрылымның қауіпсіздігін күшейту мақсаттары қойылған. Осы контексте ІІО қызметіне ЖИ енгізу – тек техникалық жаңғырту ғана емес, сонымен қатар басқару мәдениетін, шешім қабылдау жүйесін және қылмыспен күрес парадигмасын түбегейлі өзгертетін қадам болып табылады.

ЖИ технологияларын құқық қорғау саласында қолдану тек тиімділікті арттырумен шектелмейді. Бұл үдеріс белгілі бір құқықтық, этикалық және ұйымдастырушылық қиындықтарды да туындатады. Ақпараттың құпиялылығы мен деректер қауіпсіздігін сақтау, алгоритмдердің әділдігі мен айқындылығы, адам факторының сақталуы сияқты мәселелер осы бағыттағы негізгі зерттеу нысандарының бірі болып отыр.

Осылайша, ІІО қызметінде ЖИ пайдалану – қылмыстық процестердің тиімділігін арттырумен қатар, қоғамдағы сенім деңгейін нығайтуға, деректер қауіпсіздігін қорғауға және ұлттық киберқауіпсіздікті жаңа деңгейге көтеруге бағытталған стратегиялық міндет болып табылады.

Материалдар мен әдістер

Бұл ғылыми мақала кешенді әдіснамалық тәсілге негізделіп, теориялық және эмпирикалық зерттеу әдістерінің өзара үйлесімі арқылы жүзеге асырылды. Зерттеу үдерісінде ЖИ технологияларын ІІО қызметіне енгізудің тиімділігін бағалау, оның құқық қорғау қызметінің сапалық және құрылымдық трансформациясына, сондай-ақ ұлттық киберқауіпсіздік жүйесіне ықпал ету тетіктерін айқындау басты мақсат ретінде қойылды.

Зерттеу барысында жүйелі талдау әдісі қолданылып, ЖИ технологияларын құқық қорғау саласында пайдалану үрдістері мен олардың институционалдық деңгейдегі әсері кешенді түрде зерделенді. Бұл тәсіл ІІО қызметінің құрылымдық элементтері мен ақпараттық-инновациялық процестерін өзара байланысты тұтастықта қарастыруға мүмкіндік берді.

Сонымен қатар, салыстырмалы талдау әдісі негізінде шетелдік және отандық тәжірибелер салыстырылып, ІІО қызметінде ЖИ қолданудың тиімді үлгілері, ұйымдастырушылық тетіктері мен регламенттік ерекшеліктері анықталды. Мұндай салыстырмалы талдау халықаралық тәжірибеден алынған озық тәсілдерді Қазақстан жағдайына бейімдеу мүмкіндігін айқындауға бағытталды.

Зерттеуде мазмұндық және нормативтік-құқықтық талдау әдістері кеңінен қолданылды. Атап айтқанда, Қазақстан Республикасының ақпараттық қауіпсіздік, дербес деректерді қорғау, цифрлық даму, жасанды интеллектіні дамыту және ІІО қызметін реттейтін нормативтік-құқықтық актілеріне жан-жақты сараптама жасалды. Бұл талдау құқықтық реттеу тетіктерінің қазіргі жай-күйін, олардың ЖИ технологияларын енгізуге дайындығын және құқықтық олқылықтар мен шектеулерді айқындауға мүмкіндік берді.

Зерттеу барысында сондай-ақ индуктивтік және дедуктивтік әдістер, логикалық және құрылымдық талдау тәсілдері қолданылды. Индуктивтік тәсіл нақты эмпирикалық материалдар негізінде жалпы заңдылықтарды тұжырымдауға мүмкіндік берсе, дедуктивтік тәсіл арқылы жалпы теориялық қағидалар ІІО қызметінің нақты тәжірибесімен салыстырыла отырып бағаланды.

Эмпирикалық зерттеу аясында ІІО қызметінде ЖИ элементтерін қолдану тәжірибесіне қатысты ашық деректер базасы, мемлекеттік бағдарламалар, салалық есептер мен халықаралық

ұйымдардың талдамалық материалдары пайдаланылды. Бұл материалдар ІІО жүйесінің цифрлық трансформациясына әсер ететін факторларды нақтылай түсіп, ЖИ енгізудің әлеуетін бағалауға негіз болды.

Жалпы алғанда, қолданылған әдіснамалық тәсілдер мен зерттеу әдістері ЖИ технологияларын құқық қорғау саласында қолданудың теориялық және практикалық аспектілерін кешенді түрде талдауға, оның тиімділігін арттырудың институционалдық шарттары мен құқықтық негіздерін анықтауға мүмкіндік берді.

Қазіргі кезеңде киберқауіптердің сипаты мен ауқымы түбегейлі өзгерді. Киберқылмыстар жеке тұлғалар мен шағын ұйымдарға бағытталған алаяқтықтан бастап, мемлекеттік инфрақұрылымдарға бағытталған күрделі, көпдеңгейлі шабуылдарға дейін өрбіді.

Сондықтан ІІО жүйесінде деректерді талдаудың автоматтандырылған әдістерін енгізу қажеттілігі туындап ЖИ технологиялары негізгі құралға айналуда. Мұндай жүйелер ірі деректер ағындарын өңдеуге, цифрлық іздерді сәйкестендіруге және ықтимал қауіптерді алдын ала болжауға мүмкіндік береді [1, 12 б.].

Халықаралық деңгейде ІІО қызметіне ЖИ енгізу үдерісі белсенді дамуда. Europol-дың «AI and Policing» есебінде ЖИ алгоритмдерінің бейнебақылау, дауыс және мәтін тану, сондай-ақ криминологиялық болжам жасау салаларында жоғары нәтижелер көрсеткені атап өтіледі [2, 15 б.]. Мысалы, Ұлыбританияда National Crime Agency (NCA) деректерді талдау орталығында қылмыстық топтардың желілік байланысын анықтау үшін нейрондық талдау жүйелерін қолданады.

Interpol мен UNICRI бірлесе әзірлеген «Responsible AI Innovation in Law Enforcement Toolkit» құжатында ЖИ қолданудың құқықтық, этикалық және басқарушылық стандарттары нақты белгіленген [1, 8 б.]. Бұл халықаралық құрал ІІО қызметінде технологияны тек тиімді емес, сонымен қатар этикалық және құқықтық тұрғыдан қауіпсіз енгізуге мүмкіндік береді.

Қазақстанда киберқауіпсіздікті қамтамасыз ету мәселелері 2023–2029 жылдарға арналған цифрлық трансформация, ақпараттық-коммуникациялық технологиялар саласын және киберқауіпсіздікті дамыту тұжырымдамасы [3] және «Киберқалқан – 2022» тұжырымдамасы арқылы жүйелі түрде реттелуде. 2023 ж. Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі ІІО құрылымдарымен бірлесіп кибершабуылдарға қарсы әрекет ету ұлттық орталығын күшейту шараларын қабылдады [4].

Алайда, ІІО құрылымдарында ЖИ құралдарын пайдалану әзірге бастапқы деңгейде. Бұл жағдай кадрлық ресурстардың жеткіліксіздігімен, деректер сапасының төмендігімен және нормативтік-құқықтық шектеулермен байланысты. «Ақпараттандыру туралы» Қазақстан Республикасының Заңының 36-бабында [5] мемлекеттік органдардың ақпараттық жүйелерін біріктіру тәртібі белгіленгенімен, нақты ЖИ алгоритмдерін қолдану аспектілері нақты көрсетілмеген.

Бұдан бөлек, «Дербес деректер және оларды қорғау туралы» Заң ЖИ қолдану кезінде жеке тұлғалардың деректерін өңдеу мен сақтау тәртібіне шектеу қояды, бұл өз кезегінде ІІО-ның талдау процесіне әсер етеді [6].

Зерттеу нәтижелері көрсеткендей, ІІО қызметінде киберқауіпсіздікті қамтамасыз етудің тиімділігін шектейтін бірқатар факторлар бар:

- Инфрақұрылымдық әлсіздік – аппараттық және бағдарламалық құралдардың ескіруі;
- Кадрлық даярлықтың жеткіліксіздігі – ІІО қызметкерлері арасында ЖИ мен Big Data технологияларын меңгерген мамандардың аздығы;
- Нормативтік-құқықтық олқылықтар – ЖИ қолданудың құқықтық реттелуі әлі қалыптасу кезеңінде.

ЖИ технологиялары – бұл автоматтандырылған жүйелер, машиналық оқыту, нейрондық желілер, табиғи тілдерді өңдеу (NLP) және үлкен деректерді талдау секілді әдістер арқылы ақпараттық кеңістікте әрекет ететін күрделі мәселелерді шешуге мүмкіндік беретін технологиялық кешен. Құқық қорғау органдарының қызметінде ЖИ технологияларының маңызы қазіргі кезде айтарлықтай артып келеді, себебі киберқылмыстардың сипаты, масштабы және күрделілігі бұрынғыдан әлдеқайда жоғары.

Киберқылмыстармен күресте қолданылатын ақпараттық ағындар өте үлкен, күрделі және кейде құрылымсыз болады – мысалы, әлеуметтік желілер жазбалары, мәтіндік чаттар, лог-

деректер, желілік трафик, бейне-аудио жазбалар. ЖИ-ның машиналық оқыту, табиғи тілдерді өңдеу (NLP) және талдаушы алгоритмдері құқық қорғау органдарына осы деректерді автоматты түрде өңдеуге, шабуыл паттерндерін анықтауға және болжам жасауға мүмкіндік береді [7].

ЖИ алгоритмдері өткен деректерге негізделген заңдылықтарды анықтай отырып, болашақта болуы мүмкін қауіптер мен шабуылдарды болжауға қызмет етеді. Бұл құқық қорғау органдарын тек жедел жауап беру функциясынан – алдын алу функциясына қарай жылжытып отыр [8]:

- Аномалия анықтау жүйелері – ЖИ-мен жабдықталған жүйелер дәстүрлі сигнатураларға қарағанда жаңа және белгісіз шабуылдарды да табуға қабілетті [9];
- OSINT (Open Source Intelligence) құралдарында ЖИ-ны пайдалану – әлеуметтік желілердегі қылмыстық топтардың желісін анықтау, чат-боттар арқылы алдау әрекеттерін модельдеу;
- Әлеуметтік инженерия мен deepfake-қа қарсы жүйелер – генеративті модельдерді танитын және шабуыл жасаушы модульдерді бейтараптайтын шешімдер.

ЖИ-ны енгізу құқық қорғау органдарының ұлттық деңгейден трансшекаралық ынтымақтастыққа өтуін жеңілдетеді. Мысалы, Europol Innovation Lab ЖИ-ны құқық қорғау қызметінде қолдану перспективаларын талдау үшін факторлық талдаулар мен сценарийлік модельдер ұсынады [10]. Сонымен бірге, Interpol-дың «AI Toolkit» құралы құқық қорғау органдарына ЖИ-ны енгізуге көмек ретінде қызмет етеді, технологиялық, құқықтық және этикалық компоненттерге көңіл бөледі [11].

Осы күнде қылмыскерлер бір орында тұрмайды. Олар генеративті модельдер, автоматтандырылған phishing шабуылдары, интеллектуалды боттар, клонингау және deepfake технологияларын қолданады. Бұл жағдайда құқық қорғау органдары ЖИ-ға қарсы ЖИ-ны (AI vs AI) әзірлеп, шабуылдарды автоматты түрде анықтайтын, блоктайтын және оперативті түрде жауап беретін жүйелерді енгізуі қажет [12].

ЖИ-ды құқық қорғауда қолдану кейбір мәселелерді туындатады: алгоритмдік ашықтықтың болмауы, деректер сапасының төмендігі, жеке өмір мен дербес деректерді қорғау мәселелері және құқықтық-этикалық шектеулер.

Осылайша, ЖИ технологиялары киберқылмыстармен тиімді күрестегі маңызды құралға айналуда. Бірақ олардың толық әлеуетіне жету үшін құқық қорғау органдарының басқарушылық, нормативтік, кадрлық және технологиялық жүйелері бірдей жаңартылуы қажет.

ЖИ жүйесін құқық қорғау органдарында, мысалы, Europol-да немесе басқа елдердегі ІІО-да – пайдалануға енгізу алдында негізгі қадамдар: қажеттілікті айқындау, деректер инфрақұрылымын бағалау, нормативтік базаны қарастыру сияқты жұмыстарды қамтиды. Халықаралық ұйымдар бұл кезеңде пилоттық жобалар жасау, қауіп-талдау жүргізу және тиімділік критерийлерін айқындауды ұсынады. Мысалы, Interpol / UNICRI бірлесе әзірлеген құжатында «Pilot projects for evaluation of AI in law enforcement» маңызды екені белгіленген [13].

ІІО жүйелері үшін ЖИ алгоритмдерін енгізуде деректер сапасы мен қолжетімділігі басты рөл атқарады. Деректер құрылымды болуы, ал алгоритмдер бейімделіп оқытылатын болуы тиіс. Сонымен қатар алгоритмдік әділдік, айқындық, жауапкершілік талаптары қарастырылады.

ЖИ-ны толық енгізуден бұрын пилоттық режимде қолдану – тәуекелдерді азайту және жүйенің жұмысын бақылау үшін тиімді тәсіл. Пилоттық жобада алгоритмнің мінез-құлқын, деректердің динамикасын, қолданушы пікірлерін жинау және модельдің нақты жұмысын тексеру жүргізіледі.

ІІО жүйесіне ЖИ енгізу басқарушылық, нормативтік-құқықтық, кадрлық аспектілерді қамтиды. Осындай механизмдерге: ЖИ қолдану қағидаларын бекіту, алгоритмдердің ашықтығы мен жауапкершілігін қамтамасыз ету, ішкі бақылау жүйесін құру, қызметкерлерді оқыту жатады.

ЖИ енгізуі – тек технологияны орнату емес, қызметкерлердің дайындық деңгейін көтеруді, ұйымдық мәдениетті өзгерту мен жаңа жұмыс үрдістерін қалыптастыруды талап етеді. ІІО-ларда аналитиктер, ІТ-мамандар мен тергеушілер ЖИ құралдарын үйлестіріп жұмыс істеу қабілетін меңгеруі тиіс. Сонымен бірге, азаматтық сенімді нығайту үшін қоғамдық түсініктік пен диалог жүргізу маңызды [14].

ЖИ жүйесін енгізу аяқталғаннан кейін оның нәтижелілігін бағалау тетіктері қажет: алгоритмдердің әсерін өлшеу, жан-жақты тәуекелдерді қайта қарау, этикалық және құқықтық сәйкестікті үнемі тексеру. Бұл – жүйені уақыт өте келе жетілдіруін және жаңа қауіптерге бейімделуін қамтамасыз етеді.

Жасанды интеллектіні (ЖИ) құқық қорғау саласында қолдану мәселесіне арналған ғылыми және халықаралық зерттеулер соңғы жылдары айтарлықтай қарқын алды. Әлемдік ғылыми қауымдастықта ЖИ технологияларының қауіпсіздік, құқықтық реттеу және этикалық аспектілерін талдау бағытында бірқатар еңбектер жарық көрді.

Europol-дың «AI and Policing» атты баяндамасында [2, 15 б.] ЖИ алгоритмдерінің құқық қорғау жүйесіндегі тиімділігі нақты мысалдар арқылы сипатталады. Бұл есепте бейнебақылау жүйелерін интеллектуалды өңдеу, дауыс пен мәтінді тану, сондай-ақ криминологиялық болжау бағыттарындағы жетістіктер атап өтіледі. Мұндай жүйелердің көмегімен Еуропа елдерінде киберқылмыстарды анықтау уақыты қысқарып, деректерді талдау дәлдігі артқаны көрсетілген.

Interpol және UNICRI бірлесе әзірлеген «Responsible AI Innovation in Law Enforcement Toolkit» құжатында [1, 8 б.] ЖИ технологияларын құқық қорғау органдарына енгізу кезінде этикалық қағидаттардың маңызына ерекше назар аударылған. Құжатта «алгоритмдік әділдік», «деректер қауіпсіздігі» және «адам құқығын сақтау» принциптері халықаралық стандарт ретінде ұсынылады.

Батыс елдерінің тәжірибесіне сүйенсек, Ұлыбританияның National Crime Agency (NCA) құрылымында ЖИ жүйелері ұйымдасқан қылмыстық топтардың желілік байланысын анықтау үшін нейрондық талдау әдістерін қолданады. АҚШ-тағы Predictive Policing жобалары қылмыс ықтималдығын болжау арқылы полиция күштерін тиімді бөлуге мүмкіндік берген [7].

Қазақстан жағдайында ЖИ мен киберқауіпсіздікті қамтамасыз етуге қатысты ғылыми зерттеулер әлі қалыптасу сатысында. Дегенмен, «Цифрлық Қазақстан» [3] мемлекеттік бағдарламасы мен «Киберқалқан–2022» тұжырымдамасы ұлттық деңгейде ақпараттық қауіпсіздікті күшейту мен Ішкі істер органдарының цифрлық трансформациясын жеделдету бағыттарын нақты айқындаған.

Сонымен қатар, 2023 ж. қабылданған жаңа Кибершабуылдарға қарсы әрекет ету ұлттық орталығы туралы ережелер [4] ЖИ жүйелерін пайдалану арқылы киберқұқықбұзушылықтарды талдау және болжау тетіктерін енгізуге жол ашты.

Дегенмен, ЖИ-ды құқық қорғау қызметіне толыққанды енгізу барысында бірқатар шектеулер байқалады. Қазақстан Республикасының «Ақпараттандыру туралы» Заңы [5] мен «Дербес деректер және оларды қорғау туралы» Заңы [6] ЖИ қолдану кезінде деректердің құқықтық мәртебесін нақтыламаған. Бұл – құқықтық регламенттің жетілмегендігін көрсетеді.

Зерттелген әдебиеттер ЖИ-дың ІІО жүйесіндегі тиімділігін, сонымен қатар оның тәуекелдері мен этикалық аспектілерін тең дәрежеде қарастыру қажеттілігін айғақтайды. Авторлардың көпшілігі (Europol, Interpol, UNICRI, OECD зерттеулері) ЖИ-ды енгізу – тек технологиялық жетістік емес, сонымен бірге құқықтық және әлеуметтік жауапкершілік екенін атап өтеді. Сондықтан ЖИ технологияларын енгізу кезінде халықаралық тәжірибені ескере отырып, ұлттық құқықтық және кадрлық жүйелерді бейімдеу – ең өзекті ғылыми және практикалық міндеттердің бірі болып табылады.

Нәтижелер мен талқылау

Зерттеу нәтижелері Ішкі істер органдарының (ІІО) қызметінде ЖИ технологияларын енгізу құқық қорғау жүйесінің тиімділігін арттыруда айтарлықтай әлеуетке ие екенін көрсетті. ЖИ негізінде құрылған жүйелер киберқауіптерді автоматты түрде анықтап, талдау жүргізуге, сондай-ақ алдын алу шараларын нақты уақыт режимінде жүзеге асыруға мүмкіндік береді.

Біріншіден, ЖИ-ды пайдалану арқылы ІІО құрылымдарына тән үлкен деректер көлемін өңдеу сапасы артты. Машиналық оқыту және нейрондық желілер негізінде құрылған алгоритмдер кибершабуыл үлгілерін, шабуыл траекторияларын және цифрлық іздерді жоғары дәлдікпен сәйкестендіре алады [9]. Бұл қылмыстық процестердің жеделдігін арттырып, ресурстарды үнемдеуге жағдай жасайды.

Екіншіден, киберқылмыстармен күресте қолданылатын аномалия анықтау жүйелері жаңа және белгісіз қауіптерді дәстүрлі сигнатураларға қарағанда ертерек табуға мүмкіндік берді. Мұндай жүйелердің тиімділігі Europol және Interpol құрылымдарының тәжірибесінде дәлелденген [10, 11].

Үшіншіден, OSINT (Open Source Intelligence) технологияларын ЖИ-мен ұштастыру әлеуметтік желілер мен ашық деректердегі күдікті белсенділікті бақылауға мүмкіндік береді. Бұл тәсіл киберқылмыстық топтардың байланыс арналарын, жалған аккаунттар мен фишингтік шабуыл үлгілерін ерте анықтауға мүмкіндік берді [12].

Төртіншіден, зерттеу ІІО жүйесінде кадрлық және нормативтік кедергілер бар екенін көрсетті. Қызметкерлердің ЖИ мен Big Data технологияларын меңгеру деңгейі жеткіліксіз, ал заңнамалық негіз алгоритмдік ашықтық пен жауапкершілік тетіктерін толық реттемейді. Бұл жағдай ЖИ технологияларын тек техникалық емес, институционалдық тұрғыдан енгізу қажеттілігін көрсетеді.

Бесіншіден, халықаралық ұйымдардың ұсынымдарына сәйкес ІІО жүйесіне ЖИ енгізу үш кезеңнен тұруы тиіс:

1. Пилоттық жоба кезеңі – алгоритмнің тиімділігін, этикалық сәйкестігін және қауіпсіздігін тексеру.

2. Құқықтық және техникалық үйлестіру кезеңі – деректер инфрақұрылымын, нормативтік-құқықтық базаны бейімдеу.

3. Толық енгізу және бағалау кезеңі – нәтижелілікті бағалау, жүйені жетілдіру және тәуекелдерді азайту.

Зерттеу нәтижелерін талқылай келе, ЖИ технологияларын ІІО қызметіне енгізу тек киберқауіпсіздікті күшейтумен шектелмей, құқық қорғау қызметінің жаңа сапалық деңгейіне шығуға мүмкіндік беретіні анықталды. Бұл бағытта басты назар үш стратегиялық компонентке аударылуы тиіс:

- құқықтық қамтамасыз ету;
- қадрлық әлеуетті дамыту;
- қоғамдық сенім мен ашықтық.

Сонымен қатар, зерттеу нәтижелері ЖИ шешімдерінің тиімділігі ІІО-ның деректерді басқару инфрақұрылымына тікелей байланысты екенін көрсетті. Орталықтандырылған деректер платформаларының болмауы, ведомствоаралық үйлестірудің жеткіліксіздігі және деректер сапасының біркелкі еместігі алгоритмдердің жұмыс дәлдігіне әсер ететін шектеуші факторлар ретінде айқындалды. Сондықтан ЖИ жүйелерін енгізу процесінде деректер сапасын стандарттау, бірыңғай ақпараттық кеңістік қалыптастыру және киберқауіпсіздік протоколдарын жетілдіру шешуші рөл атқарады.

Талдау көрсеткендей, ЖИ технологияларын жедел-іздестіру, тергеу және профилактикалық қызметке интеграциялау құқық қорғау жүйесінің операциялық тиімділігін арттырып қана қоймай, қауіп-қатерлерді басқарудың болжамдық моделіне көшуге мүмкіндік береді. Бұл өз кезегінде ІІО қызметін реактивті тәсілден проактивті модельге көшірудің стратегиялық маңызын дәлелдейді.

Жалпы алғанда, ЖИ-дың ІІО қызметіндегі әлеуетін толық іске асыру үшін технологиялық жаңғыртумен қатар институционалдық тұрақтылық, заңнамалық айқындық және адами капиталды жүйелі дамыту талап етіледі. Осындай кешенді тәсіл ғана құқық қорғау органдарының цифрлық эволюциясына негіз бола отырып, заманауи киберқауіптерге қарсы тұру қабілетін арттыра алады.

Қорытынды

Қазіргі кезеңдегі ақпараттық-технологиялық серпін мен цифрлық трансформация қоғам өмірінің барлық саласына еніп, құқық қорғау органдарының қызметіне түбегейлі жаңа талаптар қоюда. Әсіресе киберқылмыстардың күрделенуі, ұйымдасқан қылмыстық топтардың анонимді және трансшекаралық сипат алуы Ішкі істер органдарының дәстүрлі тәсілдерінің тиімділігін төмендетіп, жаңа буындағы интеллектуалды технологиялық шешімдерді қажет етуде. Осы тұрғыдан алғанда, ЖИ технологияларын ІІО қызметіне енгізу – бұл тек инновациялық жаңашылдық емес, ұлттық және қоғамдық қауіпсіздіктің жаңа парадигмасын айқындайтын стратегиялық және жүйелік бағыт болып табылады.

Біріншіден, ЖИ технологиялары киберқылмыстарға қарсы іс-қимылда жедел талдау, үлкен деректер негізінде болжамдық модельдерді құру және қылмыстық тәуекелдерді алдын

ала анықтау арқылы құқық қорғау қызметінің тиімділігін айтарлықтай арттырады. Бұл тәсіл ІІО жүйесінде деректерге негізделген басқару мәдениетін қалыптастырып, шешім қабылдауда дәлдік пен жеделдікті қамтамасыз етеді.

Екіншіден, тергеу және жедел-іздестіру қызметтерінде ЖИ-дың енгізілуі Big Data, машиналық оқыту, бейне және мәтіндік талдау, автоматтандырылған тану және үлгілеу құралдарын кеңінен пайдалануға мүмкіндік береді. Бұл өз кезегінде жедел ақпараттық ағындарды өңдеу сапасын арттырып, тергеу мен дәлелдеу процесін ғылыми-техникалық деңгейге көтереді.

Үшіншіден, ІІО жүйесіне ЖИ технологияларын енгізу құқықтық және этикалық жауапкершілік тетіктерін жетілдіруді қажет етеді. Алгоритмдердің әділдігі, ашықтығы мен түсіндірмелілігін қамтамасыз ету, шешім қабылдау процесінде адамдық бақылауды сақтау – азаматтардың құқықтарын қорғау мен қоғамдық сенімді нығайтудың басты шарты.

Төртіншіден, ЖИ-ды енгізу тек технологиялық жаңару емес, сонымен қатар ұйымдық, кадрлық және мәдени трансформация үдерісі болып табылады. Сол себепті ІІО қызметкерлерін цифрлық сауаттылыққа, алгоритмдік ойлауға, деректермен және интеллектуалды жүйелермен өзара әрекеттесуге бейімдеу – стратегиялық маңызы бар міндет.

Сонымен қатар, ЖИ технологияларын тиімді енгізу мемлекеттік құрылымдар, ғылыми ұйымдар және жеке сектор арасындағы интеграцияны талап етеді. Мұндай көпдеңгейлі кооперация Қазақстанда да қалыптасып келе жатқан ғылыми-инновациялық экожүйенің дамуына серпін береді.

ЖИ технологияларын құқық қорғау қызметінде қолдану ІІО жүйесінің ашықтығы мен тиімділігін арттырып қана қоймай, азаматтардың қауіпсіздігі мен құқықтарының қорғалуын сапалық жаңа деңгейге көтеруге мүмкіндік береді. Алайда бұл үдеріс үздіксіз мониторингті, тәуекелдерді бағалауды және халықаралық этикалық стандарттарға сәйкестікті сақтауды талап етеді.

Жалпы алғанда, ІІО жүйесіне ЖИ технологияларын кешенді енгізу:

- киберқылмыстардың алдын алу мен ашу тиімділігін еселеп арттырады;
- тергеу және талдау процестерін интеллектуалдық автоматтандыруға мүмкіндік береді;
- ресурстарды оңтайлы және дәл бөлуді қамтамасыз етеді;
- азаматтардың жеке деректері мен құқықтарының қорғалуын жаңа деңгейге шығарады.

Болашақта ІІО қызметінде ЖИ технологияларын жүйелі түрде пайдалану Қазақстан Республикасының «Цифрлық мемлекет» тұжырымдамасымен, сондай-ақ Ұлттық киберқауіпсіздік тұжырымдамасымен үйлесімді дамуы қажет. Бұл бағыттағы ғылыми-тәжірибелік ізденістер, халықаралық ынтымақтастық және инновациялық жобаларды іске асыру ІІО қызметінің интеллектуалды әлеуетін арттырып, ұлттық қауіпсіздік жүйесінің тұрақтылығы мен сенімділігін жаңа сапалық деңгейге көтереді.

Сонымен бірге, ЖИ технологияларын енгізу барысында нормативтік-құқықтық базаны кезең-кезеңімен жаңғырту да ерекше маңызға ие. Алгоритмдер жұмысының регламенттері, деректерді жинау мен өңдеу шектері, цифрлық дәлелдемелердің процессуалдық мәртебесі сияқты мәселелер нақты құқықтық бекітуді қажет етеді. Бұл ІІО жүйесінің цифрлық трансформациясы құқықтық айқындық пен тұрақтылық негізінде жүзеге асуына жағдай жасайды.

Қорытындылай келе, ЖИ-ды құқық қорғау саласына енгізу – тек техникалық жаңғыру емес, сонымен қатар басқару мәдениетін, кәсіби стандарттарды және қылмыспен күрес стратегиясын жаңаша түсіндіруді қажет ететін күрделі көпфакторлы процесс. Осы бағыттағы үйлесімді саясат, кадрлық әлеуетті дамыту және ғылыми-техникалық прогресті уақытылы институционализациялау ІІО қызметінің тиімділігін арттырып, заманауи қауіп-қатерлерге қарсы тұра алатын орнықты және интеллектуалды құқық қорғау жүйесін қалыптастыруға мүмкіндік береді.

ӘДЕБИЕТТЕР

1 Responsible AI Innovation in Law Enforcement Toolkit // United Nations Interregional Crime and Justice Research Institute. 2024. P. 8–13. URL: https://unicri.org (accessed: 12.10.2025)

2 AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement. The Hague: European Union Agency for Law Enforcement Cooperation. URL: https://www.europol.europa.eu (accessed: 10.10.2025)

3 2023–2029 жылдарға арналған цифрлық трансформация, ақпараттық-коммуникациялық технологиялар саласын және киберқауіпсіздікті дамыту тұжырымдамасын бекіту туралы: Қазақстан Республикасы Үкіметінің 2023 жылғы 28 наурыздағы № 269 қаулысы. URL: https://adilet.zan.kz/kaz/docs/P2300000269/history (өтініш берілген күн: 10.10.2025)

4 Кибершабуылдарға қарсы әрекет ету ұлттық орталығын күшейту туралы: баспасөз ақпараты. – Астана, 2025. URL: https://www.gov.kz (өтініш берілген күн: 10.10.2025)

5 Ақпараттандыру туралы: Қазақстан Республикасының 2015 жылғы 24 қарашадағы № 418-V ҚРЗ Заңы. URL: https://www.adilet.zan.kz (өтініш берілген күн: 10.10.2025)

6 Дербес деректер және оларды қорғау туралы: Қазақстан Республикасының 2013 жылғы 21 мамырдағы № 94-V Заңы. URL: https://www.adilet.zan.kz (өтініш берілген күн: 10.10.2025)

7 Қылмыспен күресте жасанды интеллект әдістерін қолдану // Russian Law Journal. – № 12 (2). URL: https://www.russianlawjournal.org.

8 Құқық қорғау органдарындағы жасанды интеллект: заңсыз ақша ағындарын бұзуға арналған жасанды интеллект шешімдері // eucrim – The European Criminal Law Associations' Forum. 2023. No. 1. P. 60–66. URL: https://eucrim.eu (accessed:: 11.10.2025)

9 Цифрлық Әлемнің қауіпсіздігін қамтамасыз ету: жасанды интеллект (AI) қолдайтын зиянды бағдарламалар мен интрузияны анықтау арқылы интеллектуалды инфрақұрылымдар мен цифрлық индустрияларды қорғау. URL: https://arxiv.org (өтініш берілген күн: 10.10.2025)

10 Жасанды интеллект және полиция қызметі: жасанды интеллекттің құқық қорғау органдары үшін артықшылықтары мен қиындықтары // Luxembourg: Publications Office of the European Union. URL: https://op.europa.eu (өтініш берілген күн: 12.10.2025)

11 Құқық қорғау органдарындағы жасанды интеллекттің жауапты инновацияларына арналған құралдар жинағы. – Lyon: INTERPOL. URL: https://www.interpol.int (өтініш берілген күн: 10.10.2025)

12 Жасанды интеллектті өзгерту: Еуропол ауыр ұйымдасқан қылмыс пен терроризммен күресу үшін жасанды интеллектті қалай пайдаланады // Академиялық журнал. – 2023. – № 72(9). URL: https://belugyiszemlejournal.org (өтініш берілген күн: 10.10.2025)

13 Principles for Responsible AI Innovation in Law Enforcement. URL: https://ai-lawenforcement.org (accessed: 10.10.2025)

14 Application of AI in Law Enforcement and Crime Prevention: MNU Research-Based Evaluation Enhances the Legislative Process in Kazakhstan. URL: https://mnu.kz/news (accessed: 10.10.2025)

REFERENCES

1 Responsible AI Innovation in Law Enforcement Toolkit // United Nations Interregional Crime and Justice Research Institute. 2024. P. 8–13. URL: https://unicri.org (accessed: 12.10.2025). (In English)

2 AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement. The Hague: European Union Agency for Law Enforcement Cooperation. URL: https://www.europol.europa.eu (accessed: 10.10.2025). (In English)

3 2023–2029 jyldarğa arnalğan sifrlyq transformasia, aqparattyq-komunikasialyq tehnologialar salasyn jäne kiberqauıpsızdıktı damytu tūjyrymdamasyn bekıtu turaly: Qazaqstan Respublikasy Ükımetınıñ 2023 jylğy 28 nauryzdağy No. 269 qaulysy. URL: https://adilet.zan.kz/kaz/docs/P2300000269/history (ötınış berılgen kün: 10.10.2025). (In Kazakh)

4 Kiberşabuyldarğa qarsy äreket etu ūlttyq ortalyğyn küşeitu turaly: baspasöz aqparaty. Astana. URL: https://www.gov.kz (ötınış berılgen kün: 10.10.2025). (In Kazakh)

5 Aqparattandyru turaly: Qazaqstan Respublikasynyñ 2015 jylğy 24 qaraşadağy № 418-V QRZ Zañy. URL: https://www.adilet.zan.kz (ötınış berılgen kün: 10.10.2025). (In Kazakh)

6 Derbes derekter jäne olardy qorğau turaly: Qazaqstan Respublikasynyñ 2013 jylğy 21 mamyrdağy № 94-V Zañy. URL: https://www.adilet.zan.kz (ötınış berılgen kün: 10.10.2025). (In Kazakh)

7 Qylmyspen küreste jasandy intelekt ädısterın qoldanu // Russian Law Journal. No. 12(2). URL: https://www.russianlawjournal.org. (In Kazakh)

8 Qūqyq qorğau organdaryndağy jasandy intelekt: zañsyz aqşa ağyndaryn būzuğa arnalğan jasandy intelekt şeşımderı // eucrim – The European Criminal Law Associations' Forum. 2023. No. 1. P. 60–66. URL: https://eucrim.eu (accessed: 11.10.2025). (In Kazakh)

9 Sifrlyq Älemnıñ qauıpsızdıgın qamtamasyz etu: Jasandy intelekt (AI) qoldaityn ziandy bağdarlamalar men intruziany anyqtau arqyly intelektualdy infraqūrylymdar men sifrlyq industrialardy qorğau. URL: https://arxiv.org (ötınış berılgen kün: 10.10.2025). (In Kazakh)

10 Jasandy intelekt jäne polisia qyzmetı: jasandy intelekttıñ qūqyq qorğau organdary üşın artyqşylyqtary men qiyndyqtary. Luxembourg: Publications Office of the European Union. URL: https://op.europa.eu (ötınış berılgen kün: 12.10.2025). (In Kazakh)

11 Qūqyq qorğau organdaryndağy jasandy intelekttıñ jauapty innovasialaryna arnalğan qūraldar jinağy. Lyon: INTERPOL. URL: https://www.interpol.int (ötınış berılgen kün: 10.10.2025). (In Kazakh)

12 Jasandy intelekttı özgertu: Europol auyr ūiymdasqan qylmys pen terorizmmen küresu üşın jasandy intelekttı qalai paidalanady // Akademialyq jurnal. 2023. No. 72(9). URL: https://belugyiszemlejournal.org (ötınış berılgen kün: 10.10.2025). (In Kazakh)

13 Principles for Responsible AI Innovation in Law Enforcement. URL: https://ai-lawenforcement.org (accessed: 10.10.2025). (In English)

14 Application of AI in Law Enforcement and Crime Prevention: MNU Research-Based Evaluation Enhances the Legislative Process in Kazakhstan. URL: https://mnu.kz/news (accessed: 10.10.2025). (In English)

АПАХАЕВ Н.Ж.,*[1]
к.ю.н., профессор.
*e-mail: apahaev_nurlan@mail.ru
ORCID ID: 0000-0001-7795-2518
ЗУЛЕЕВА А.Ж.,[1]
PhD, ассоциированный профессор.
e-mail: ainagul.z@mail.ru
ORCID ID: 0009-0003-1049-6038
ШИДЕМОВ А.Г.,[1]
PhD, ассоциированный профессор.
e-mail: Sh_azem@mail.ru
ORCID ID: 0009-0001-8643-4058
[1]Q University,
г. Алматы, Казахстан

МЕХАНИЗМЫ ПОВЫШЕНИЯ КИБЕРБЕЗОПАСНОСТИ ПУТЕМ ВНЕДРЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ДЕЯТЕЛЬНОСТЬ ОВД

Аннотация

В настоящее время технологии искусственного интеллекта становятся катализатором кардинальных изменений в правоохранительной сфере. Усложнение киберпреступлений, обретение трансграничного характера и рост преступной активности в цифровом пространстве требуют применения органами внутренних дел новых подходов и инструментов. В данной статье подробно рассмотрены основные механизмы внедрения искусственного интеллекта в деятельность ОВД, его роль в обеспечении кибербезопасности и институциональные, правовые и технические аспекты практической реализации. В ходе исследования был проведен анализ стратегических документов и рекомендаций международных организаций Interpol, Europol, UNICRI и OECD, а также национальных стратегий цифровизации и кибербезопасности Республики Казахстан. В ходе исследования были изучены особенности и преимущества применения ИИ в деятельности ОВД на основе метода системного анализа, сопоставления зарубежного и отечественного опыта с целью оценки эффективности внедрения ИИ в деятельность ОВД и определения его влияния на систему кибербезопасности.

Ключевые слова: искусственный интеллект, кибербезопасность, киберпреступность, анализ данных, машинное обучение, цифровизация, правовое регулирование.

APAKHAEV N.ZH.,*[1]
c.l.s., professor.
*e-mail: apahaev_nurlan@mail.ru
ORCID ID: 0000-0001-7795-2518
ZULEEVA A.ZH.,[1]
PhD, associate professor.
e-mail: ainagul.z@mail.ru
ORCID ID: 0009-0003-1049-6038
SHIDEMOV A.G.,[1]
PhD, associate professor.
e-mail: Sh_azem@mail.ru
ORCID ID: 0009-0001-8643-4058
[1]Q University,
Almaty, Kazakhstan

MECHANISMS FOR INCREASING CYBERSECURITY THROUGH THE INTRODUCTION OF ARTIFICIAL INTELLIGENCE IN THE ACTIVITIES OF THE DEPARTMENT OF INTERNAL AFFAIRS

Abstract

Currently, artificial intelligence technologies are becoming a catalyst for radical changes in the field of law enforcement. The complication, transboundary nature of cybercrime and the increase in criminal activity in the digital space require the use of new approaches and tools by the internal affairs bodies. In this article, the main mechanisms for introducing artificial intelligence into the activities of the Department of internal affairs, its role in ensuring cybersecurity and institutional, legal and technical aspects of practical implementation are considered in detail. The study analyzed the strategic documents and recommendations of international organizations Interpol, Europol, UNICRI and OECD, as well as the National digitalization and cybersecurity strategies of the Republic of Kazakhstan. In the course of the study, in order to assess the effectiveness of the introduction of AI into the activities of the IAB and determine its impact on the cybersecurity system, the features and advantages of the use of AI in the activities of the IAB were studied on the basis of a systematic analysis method, a comparison of foreign and domestic experience.

Keywords: artificial intelligence; cybersecurity; cybercrime; data analytics; machine learning; digital transformation; legal regulation.

Мақаланың редакцияға түскен күні: 30.10.2025