МРНТИ: 28.23.19 https://doi.org/10.65247/3105-3432-2025-4.03

КИБЕРҚАУІПТЕРДІ АНЫҚТАУДА ЖӘНЕ АЛДЫН АЛУДА ЖАСАНДЫ ИНТЕЛЛЕКТТІ ПАЙДАЛАНУ

*[1]Д.НСАНБАЕВ, [1]Ш.К.ЕЛЕЖАНОВА
[1]Х.Досмухамедов атындағы Атырау университеті
(Атырау, Қазақстан)
*nsanbaev.15@gmail.com, 200103419@stu.sdu.edu.kz

Аңдатпа
Бұл мақалада киберқауіптерді анықтау және алдын алу мақсатында жасанды интеллект (ЖИ) технологияларын қолдану зерттеледі. Сандық дәуірдің дамуымен қатар, кибершабуылдардың саны мен күрделілігі артуда. Дәстүрлі әдістер бұл қауіптерге қарсы тұруда жиі жеткіліксіз болып жатады, сондықтан заманауи тәсілдерді енгізу қажеттілігі туындайды. ЖИ технологиялары үлкен көлемдегі деректерді жылдам өңдеу, аномалияларды анықтау және шабуылдарға алдын ала жауап беру қабілеті арқылы киберқауіпсіздікті жаңа деңгейге көтеруге мүмкіндік береді. Мақаланың негізгі мақсаты – ЖИ технологияларын қолданудың тиімділігін бағалау және олардың қазіргі заманғы киберқауіпсіздік жүйелерінде пайдалану жолдарын ұсыну. Зерттеу барысында машиналық оқыту алгоритмдері мен деректерді өңдеу әдістері қолданылып, олардың шабуылдарды анықтаудағы дәлдігі мен жылдамдығы талданды. Алынған нәтижелер ЖИ құралдарының дәстүрлі әдістермен салыстырғанда жоғары тиімділігін көрсетті. Бұл жұмыс киберқауіпсіздік саласындағы зерттеулерге қосымша үлес қосып, ақпараттық инфрақұрылымды қорғаудың жаңа мүмкіндіктерін ашуға бағытталған. Сонымен қатар, мақалада осы әдістерді енгізу барысында кездесуі мүмкін қиындықтар мен оларды шешу жолдары талқыланады.
Түйін сөздер: киберқауіптер, жасанды интеллект, деректерді талдау, машиналық оқыту, аномалияларды анықтау, ақпараттық қауіпсіздік.

Кіріспе

Ақпараттық технологиялардың (IT) дамуы киберқылмыстардың көбеюіне әкеліп соқты, себебі қылмыскерлер киберкеңістікті өз мақсаттарына пайдаланып жатыр. Күрделі таратылған және интернет-компьютинг жүйелерінің даму үрдістері ақпараттық қауіпсіздік пен жеке деректердің құпиялығы туралы маңызды сұрақтарды көтеруде. Киберинфрақұрылымдар бұзушылықтар мен басқа да қауіп-қатерлерге өте осал. Физикалық құрылғылар, мысалы, сенсорлар мен детекторлар, бұл инфрақұрылымдарды бақылау және қорғау үшін жеткіліксіз, сондықтан қалыпты мінез-құлықтарды модельдейтін және аномалияларды анықтай алатын жетілдірілген IT жүйелер қажет. Мұндай киберқорғаныс жүйелері икемді, бейімделгіш және тұрақты болуы керек, сондай-ақ қауіптердің әртүрлі түрлерін анықтап, нақты уақыт режимінде ақылды шешімдер қабылдай алуы тиіс [Chen H., Wang F.Y., 2005: 12-16 бб.].

Кибершабуылдардың жылдамдығы мен санының артуына байланысты шабуылдарды уақытылы талдау және оларға дұрыс жауап беру үшін тек адам араласуы жеткіліксіз. Көптеген желіге бағытталған кибершабуылдар компьютерлік құрттар мен вирустар сияқты интеллектуалды агенттер арқылы жүзеге асады; сондықтан олармен күресу үшін кибершабуылдарды анықтайтын, бағалайтын және жауап қайтаратын интеллектуалды жартылай автономды агенттерді пайдалану қажеттілігі туындап отыр. Бұл «компьютерлік жасақтар» шабуыл түрін, оның мақсатын және оған қарсы қандай әрекет қолдану керектігін, сондай-ақ екінші деңгейлі шабуылдардың алдын алу әдістерін жылдам анықтай алуы тиіс [Stytz M.R. et al., 2005].

Сонымен қатар, кибершабуылдар тек белгілі бір аймақтармен шектелмейді. Олар әлемдік деңгейде барлық компьютерлік жүйелерге қауіп төндіреді және бұл қауіп күн сайын артып келеді. Бұрын киберқылмыстарды тек білімді мамандар жасай алатын болса, бүгінде интернеттің кеңеюімен кез келген адам мұндай қылмыстарды жасау үшін қажетті білім мен

құралдарға қол жеткізе алады. Шешім қабылдау деңгейіндегі дәстүрлі қатаң бекітілген алгоритмдер динамикалық өзгеретін кибершабуылдарға қарсы тұруда тиімсіз болып қалды. Сол себепті бағдарламалық жасақтамаға икемділік пен үйрену қабілетін беретін жасанды интеллект (ЖИ) әдістерін қолдану қажеттілігі туындап отыр [Helano J., Nogueira M., 2006: 28-32 бб.].

ЖИ осы және басқа да мүмкіндіктерді ұсынады. ЖИ-дың табиғаттан шабыттанған есептеу әдістері (мысалы, есептеу интеллекті, нейрондық желілер, интеллектуалды агенттер, жасанды иммундық жүйелер, машиналық оқыту, деректерді өңдеу, үлгілерді тану, бұлыңғыр логика, эвристикалық тәсілдер және т.б.) киберқылмыстарды анықтау мен алдын алуда маңызды рөл атқаруда. ЖИ өз қолдану контекстіне бейімделетін, өзін-өзі басқару, өзін-өзі баптау, өзін-өзі конфигурациялау, өзін-өзі диагностика жасау және өзін-өзі қалпына келтіру әдістерін пайдаланатын автономды есептеу шешімдерін жасауға мүмкіндік береді. Ақпараттық қауіпсіздіктің болашағы тұрғысынан қарағанда, ЖИ әдістері киберкеңістікті қорғау шараларын жетілдіруге бағытталған перспективалық зерттеу саласы болып табылады [Dasgupta D., 2006: 2-3 бб.].

Бұл зерттеудің мақсаты – киберқылмыстармен күресуде қолданылған ЖИ әдістерінің қазіргі жетістіктерін көрсету, олардың кибершабуылдарды анықтау мен алдын алуда тиімді құрал бола алатынын көрсету және болашақ зерттеулерге жол ашу.

Негізгі бөлім

Жасанды интеллект (ЖИ) технологиясының әлемдік деңгейде енгізілуі әртүрлі салаларға оң және теріс әсерін тигізуде. Бұл технология көптеген салаларда, соның ішінде киберқауіпсіздікте де үлкен жетістіктерге қол жеткізді. Perols және Murthy зерттеулеріне сәйкес, жасанды интеллект бизнес пен компанияларға айтарлықтай әсер етті. Алайда, жасанды интеллекттің киберқауіпсіздікке тигізетін әсері екі жақты: бір жағынан, ол жүйелердің қорғанысын күшейтсе, екінші жағынан, хакерлерге жаңа шабуыл тәсілдерін дамытуға мүмкіндік береді [Perols R., Murthy U., 2018].

Компанияларға жасалатын кибершабуылдар барған сайын қауіпті бола түсуде. Шабуылдаушылар киберқауіпсіздік технологияларындағы осалдықтарды табу үшін білімдерін жетілдіруде. Дегенмен, машинамен оқыту алгоритмдері шабуылдаушылардың бірдей әдістерді қолдана алмауын қамтамасыз етеді. Жасанды интеллекттің негізгі артықшылықтарының бірі – жүйелік қателерді болдырмау. Бұл технология киберқауіпсіздік саласындағы маңызды артықшылықтар қатарын қамтамасыз етеді.

Әлемдегі көптеген ұйымдар құпия ақпаратты қорғауға мұқтаж. Жасанды интеллект болашақта осы қажеттілікті қанағаттандыру үшін кеңінен дамытылады. Киберқауіпсіздікке енгізілген жасанды интеллект жүйелері шабуыл әрекеттерін анықтап, олардан үйрене алады. Бұл технологияның негізгі ерекшеліктерінің бірі – тәжірибеден үйрену қабілеті. Жасанды интеллект алгоритмдері бұрын орын алған оқиғалардан сабақ алып, кибершабуылдарды болдырмауға мүмкіндік береді.

Жасанды интеллект - қазіргі заманның ең күрделі технологияларының бірі. Ол деректерді өңдеу жылдамдығын арттырып, жүйелерді жетілдіруге ықпал етеді. Сонымен қатар, жасанды интеллект киберқылмысты азайтуға көмектеседі. Оның мониторинг жүргізу қабілеті адамның мүмкіндіктерінен әлдеқайда жоғары болғандықтан, жүйедегі ақауларды жылдам анықтауға мүмкіндік береді. Бұл - ұйымдардың қауіпсіздік хаттамаларын күшейтіп, деректерін қорғауына септігін тигізетін маңызды фактор.

ЖИ технологиясы деректерді шифрлеу және қорғау шараларын жетілдіруге де үлес қосты. Деректер - кез келген бизнес үшін маңызды ресурс, сондықтан олардың қауіпсіздігін қамтамасыз ету қажет. Түрлі шифрлеу хаттамаларының көмегімен жасанды интеллект жүйелері деректерді қауіпсіз сақтау үшін күрделі шифрлеу механизмдерін қолданады.

Дегенмен, жасанды интеллекттің кеңінен енгізілуі киберқауіпсіздік саласындағы кейбір

жұмыс орындарының қысқаруына әкелді. Себебі бұл технология адам қызметін тиімді алмастырып, киберқауіпсіздік мамандарының рөлін азайтуда. Сонымен қатар, ЖИ технологиясы жүйенің техникалық қызмет көрсету қажеттілігін төмендетеді, өйткені ол өзін-өзі оңтайландыру және жүйені терең түсіну қабілетіне ие.

N.Mengidis және басқалардың зерттеулері көрсеткендей, жасанды интеллект оқыту жүйелерін киберқауіпсіздікке енгізу жүйеге шабуылдарды болдырмауға көмектеседі. Мұндай жүйелер хакерлердің әрекеттерін талдап, жаңа қорғаныс механизмдерін автоматты түрде әзірлейді. Осы фактордың арқасында шабуылдаушылар қажетті ақпаратқа қол жеткізе алмайды. Жасанды интеллекттің тиімділігін арттыратын бірнеше әдістер бар [Mengidis N. et al., 2019].

Қолтаңбаға негізделген әдістер

Жасанды интеллекттің киберқауіпсіздікке әсерінің бірі – қолтаңбаға негізделген әдістерді қолдану. Бұл әдіс ЖИ-дің кибершабуылдар мен зиянды бағдарламалардың кодтарын анықтауына мүмкіндік береді. Жасанды интеллект зиянды бағдарламалар кодтарын дерекқордағы белгілі шабуыл кодтарымен салыстырып, сәйкестікті анықтайды. Бұл әдістің негізгі артықшылығы – ол шабуылды тез анықтауға және алдын алуға көмектеседі [Chung S., 2021].

Алайда, бұл әдіс жаңа шабуыл түрлері пайда болған жағдайда тиімсіз болуы мүмкін. Егер дерекқорда жаңа зиянды код туралы ақпарат болмаса, жүйе оны анықтай алмауы ықтимал. Осыған байланысты шабуылдаушылар өздерінің шабуыл үлгілерін өзгертіп, жасанды интеллект жүйелерін айналып өту тәсілдерін ойлап табуда.

Машиналық оқыту әдісі және қаржылық алаяқтықты анықтаудың әдістері

Машиналық оқыту әдістері киберқауіпсіздікке айтарлықтай әсер етті. Mengidis және басқалардың зерттеулері көрсеткендей, адамдар деректерді талдауда қателіктер жіберуі мүмкін, ал жасанды интеллект мұндай қателіктерден аулақ бола алады. ЖИ жүйелері журналдарды, желілік пакеттерді талдап, шабуыл белгілерін автоматты түрде анықтай алады [Mengidis N. et al., 2019].

ЖИ технологиясының негізгі артықшылығы – үлкен көлемдегі деректерді талдау қабілеті. Адамдарға қарағанда, ЖИ кең ауқымды ақпаратты өңдеп, қателіктер жібермейді. Машиналық оқыту әдістері, соның ішінде кластерлеу және жіктеу, жүйедегі аномалияларды анықтауға көмектеседі. Бұл әдістер ақпараттық қауіпсіздікті қамтамасыз етуде маңызды рөл атқарады.

Қаржылық алаяқтықпен күресу үшін кешенді жүйе бірнеше маңызды қадамдарды қамтиды. Біріншіден, «Клиентіңді біл» (KYC) және «Ақшаны жылыстатуға қарсы күрес» (AML) талаптарын орындау мақсатында транзакциялық деректер жиналады. Жинақталған ақпарат алаяқтыққа қарсы бағдарламалар үшін өңделіп, белгіленеді. Бұл процесте CatBoost сияқты алгоритмдер деректерді минималды алдын ала өңдеумен жұмыс істей алады. Одан кейін XGBoost, LightGBM, CatBoost секілді машиналық оқыту (МО) модельдері таңдалып, заңды және алаяқтық операцияларды ажырату үшін оқытылады. Дайын модель тәуекелдерді анықтау мақсатында қолданылып, күмәнді транзакциялар қолмен тексеріледі. Сонымен қатар, алаяқтық белгілерін жаңарту және үздіксіз мониторинг жүргізу маңызды.

Қаржылық алаяқтықты болдырмау үшін арнайы инфрақұрылым қажет. Бұл инфрақұрылымға алаяқтыққа қарсы жұмыс істейтін сарапшылар тобы, қатаң саясаттар, тергеу және есеп беру процестері, ұйымдық хабардарлықты арттыру бойынша оқыту және қауіпсіздікке мән беретін серіктестерді таңдау кіреді. Бүгінгі таңда қаржы мекемелеріне төнетін негізгі қауіптер қатарында алаяқтық технологияларының дамуы бар. Мысалы, Deepfake технологиясы арқылы жалған аудио-видео көмегімен есепшоттарға кіру мүмкіндігі артқан. Сонымен қатар, Fraud-as-a-Service қызметтері алаяқтықты тәжірибесіз адамдарға да қолжетімді етіп отыр.

Әлеуметтік инженерия және фишинг те қаржы мекемелері үшін үлкен қауіп төндіреді. Жалған хаттар мен SMS арқылы жеке деректерді ұрлау немесе психологиялық қысым арқылы

адамдарды ақша аударуға мәжбүрлеу кең таралған әдістердің бірі. Бұдан бөлек, қайырымдылық саласындағы алаяқтық схемалары да жиі кездеседі, мұнда жалған қайырымдылық ұйымдары арқылы қаражат жымқыру әрекеттері жүзеге асады. Осындай қауіптерден қорғану үшін серіктестерді мұқият тексеру, киберқауіпсіздік бойынша оқыту бағдарламаларын жүргізу және машиналық оқыту мен транзакцияларды талдау сияқты заманауи технологияларды енгізу қажет [Тастанбеков М.Б., Омаров Б.С., 2024].

Желілік шабуылдарды анықтау жүйелері

Желілік шабуылдар - киберқауіпсіздікке жасалатын ең көп таралған қауіптердің бірі. Сондықтан желілік шабуылдарды ерте анықтау өте маңызды. Жасанды интеллектті желілік қауіпсіздік жүйелеріне енгізу арқылы бұл мәселе оңай шешіледі. AI технологиясын қолданатын желілік брандмауэрлер рұқсатсыз қолжетімділікті болдырмайды және қауіпсіздікті арттырады.

Желілік шабуылдарды анықтау жүйелері бес негізгі элементке негізделген, олардың бірі - үлкен көлемдегі деректерді талдау қабілеті. Бұл әдістер ұйымдарға желі арқылы жасалатын шабуылдарды болдырмауға және ақпараттық қауіпсіздікті қамтамасыз етуге көмектеседі.

Жасанды интеллект киберқауіпсіздік саласына үлкен ықпал етті. Ол жүйелердің қауіпсіздігін арттырып, шабуылдарды анықтау және алдын алу әдістерін жетілдіруге мүмкіндік берді. Сонымен қатар, ЖИ технологиялары кибершабуылдарға қарсы тиімді құрал ретінде дамуда. Жасанды интеллекттің киберқауіпсіздікке ықпалының артуы оның болашақта одан әрі жетілдірілетінін көрсетеді [Ansari M. et al., 2022].

Әдеби шолу

Киберқауіпсіздік шаралары бойынша NCSS зерттеу баяндамасында мемлекеттер қоғамдық ақпараттандыру, инциденттерді алдын алу және мемлекеттік-жекеменшік серіктестіктерді басым бағыт ретінде қарастыратыны көрсетілген. Дегенмен, Малайзия, Израиль және Иран сияқты елдер өздерінің белгіленген мақсаттарын толық жүзеге асырған жоқ, бұл қосымша даму мен күшті жүзеге асыру қажеттілігін көрсетеді. Ұлыбритания, АҚШ және Германия сияқты елдерде айтарлықтай жақсы саясаттар енгізілген, олар шабуылдарға қарсы қорғаныс, CERT және киберқауіпсіздік туралы ақпараттандыру шараларының маңыздылығын атап өтеді [Shafqat N., 2016]. Алайда, ақпараттық қауіпсіздік пен киберқауіпсіздік терминдері бір-бірімен ауыстырылып қолданылса да, киберқауіптер белгіленген шектерден асып түседі. Киберқауіпсіздіктің адам факторының рөлі артып келе жатқаны, өйткені адамдардың осал тұстары мен қауіптері бар; қазіргі уақытта халықаралық үздік тәжірибелер мен стандарттармен киберкеңістікті толықтай қорғау мүмкін емес [Solms R., Niekerk J., 2013].

Гелани анықтамасы бойынша, киберқауіпсіздік дегеніміз - ақпаратты, деректерді, ресурстарды, қызметтерді және құнды жүйелерді жоғалтудан, зақымданудан, бұзылудан, айыптаудан немесе теріс пайдалануынан қорғау іс-әрекеті. Бұл киберкеңістікті және киберкеңістікке негізделген жүйелерді қорғай отырып, жүйенің дұрыс басқарылуын қамтамасыз етуге бағытталған шара. Киберқауіпсіздіктің негізі - активтерді қорғау, меншік құқықтарын сақтап қалу және жүйелер мен деректерді бақылау [Ghelani D., 2022]. Киберқауіпсіздік 1990 жылдары басталған деп есептеледі, бірақ вирус пен құрттар киберкеңістіктің алғашқы кезеңдерінен бастап болды. Ғылым мен технологиядағы алға жылжумен киберқауіпсіздік 1990 жылдары үлкен серпіліс жасады [Ghate S., Agrawal P.K., 2017].

Қаржы мен киберқауіпсіздік арасындағы байланыс бизнес үшін өте маңызды бола бастады, өйткені олар өзгермелі бизнес пен технологиялық жағдайларда интегритетті, қауіпсіздікті және реттеу талаптарын сақтауды мақсат етеді [Abrahams T.O. et al., 2024]. Цифрландырудың қарқынды дамуы мен технологияның әртүрлі салаларда кеңінен қолданылуы киберқауіпсіздікке назар аударуды қажет етеді. Қызметтер мен бағдарламалық қамтамасыз етуді біріктіру арқылы ұйымдарда тиімділік пен даму мүмкіндіктері туындайды, бірақ

олардың өзара байланысы оларды кибершабуылдар мен деректердің бұзылу сияқты қауіптерге осал етеді.

Кибершабуылдардың күрделілігі артқан сайын, ұйымдарға арналған жоғары деңгейдегі киберқауіпсіздік шаралары қажет. Дәстүрлі әдістер өзгермелі зиянды бағдарламалар мен кибершабуылдарды анықтауда қиындықтар туғызады. Ұйымдар үшін тәуекелдерді басқару әдістерін кешенді талдау қажет. Заңнамаларға сәйкестікті тек сақтау емес, ұйымдар өздерінің ерекше қауіптерін анықтап, оларды басқару үшін белсенді шаралар қабылдауы тиіс.

Машиналық оқыту - жасанды интеллектінің бір бөлігі, ол деректерден үйреніп, айқын бағдарламалаусыз болжамдар жасауды қамтамасыз етеді. Қадағаланатын оқыту белгілермен деректерді пайдалана отырып алгоритмдерді оқытады, ал қадағаланбайтын оқыту белгісіз деректерден үлгілерді іздейді. Жасанды интеллектінің осы әдістері деректерді талдауға, болжауға және шешімдер қабылдауға көмектесіп, көптеген салаларда жетістіктерге жетуге мүмкіндік береді [Kumar S. et al., 2019].

Машиналық оқыту (МО) негізінде алгоритмдер жасалады, олар деректерді өңдеп, талдап, содан кейін алынған білімді шешім қабылдауға пайдаланады. Регрессиялық талдау - қадағаланатын оқытудың техникаларының бірі, ол тәуелді және тәуелсіз айнымалылар арасындағы байланыстарды зерттейді. Линейлік регрессия - қарапайым әрі жиі қолданылатын әдіс, ал логистикалық және полиномиалды регрессиялар сызықты емес қатынастарды шешуге мүмкіндік береді. МО сондай-ақ деректерді кластерлеу, өлшемділікті азайту сияқты процестерде қолданылуда.

Машиналық оқытуның пайдасы әртүрлі салаларда айқын көрінеді. Медицинада ауруларды ерте анықтауға және емдеу жоспарларын жекелендіруге мүмкіндік береді. Қаржы секторында алаяқтықты анықтауға және тәуекелдерді бағалауға қолданылады. Өздігінен басқарылатын көліктер де МО арқылы қауіпсіз навигация мен тиімді маршрут жоспарлау мүмкіндігін алады [Kanade V., 2022].

Қазақстанда жасанды интеллектті киберқауіпсіздік саласында пайдалану зерттеулері шектеулі. Осы тақырыпқа қатысты қазақстандық дереккөздер аз болғандықтан, негізінен халықаралық зерттеулерге сүйендік. Дегенмен, қаржылық алаяқтықты анықтауда машиналық оқытуды қолдану туралы кейбір отандық еңбектер бар, мысалы: Тастанбеков М.Б. және Омаров Б.С. (2024).

Әдістер

Зерттеу барысында киберқауіптерді анықтау мен алдын алуда жасанды интеллектті тиімді пайдалану үшін бірнеше әдіс қолданылды. Алдымен, саланың ағымдағы жағдайын және осы салада қолданыстағы шешімдерді зерттеу маңызды қадам болды. Бұл зерттеу жасанды интеллекттің киберқауіпсіздік саласындағы мүмкіндіктерін тереңірек түсінуге және зерттеу жұмысының бағыттарын нақтылауға мүмкіндік берді.

Әдеби шолу. Жасанды интеллекттің киберқауіптерді анықтауда қолданылуы бойынша 10-нан астам ғылыми мақала мен зерттеу жұмысы талданып, олардың ішінен бес негізгі мақала таңдалып алынды. Әр мақалада ұсынылған әдістер мен статистикалық мәліметтер негізінде зерттеудің тиімділігі бағаланды.

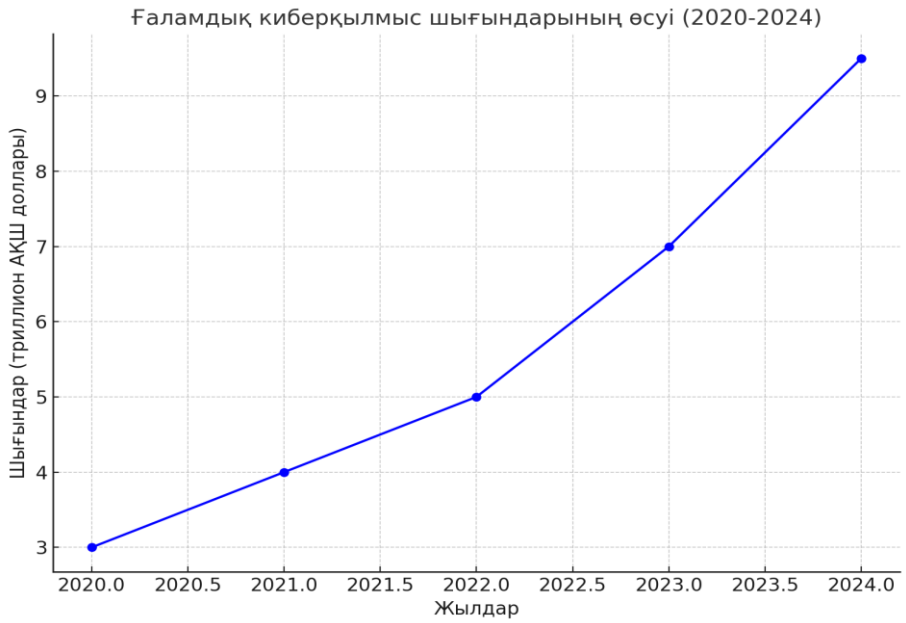
Мақалаларды салыстыру және деректерді талдау. Әр мақаладағы әдістер мен құралдар салыстырмалы түрде зерттелді. Негізгі назар жасанды интеллекттің шабуылдарды ерте анықтау және оларды болдырмау қабілетіне аударылды.

Нарықтық талдау. Киберқауіпсіздікке арналған қолжетімді құралдар мен платформалар зерттелді. Әрбір шешімнің ерекшеліктері, артықшылықтары және шектеулері қарастырылды, бұл зерттеудің инновациялық тәсілдерін анықтауға ықпал етті.

Жоғарыда аталған әдістер зерттеудің негізін қалап, нәтижелердің дәлдігі мен сенімділігін қамтамасыз етті.

Нәтижелер

Жасанды интеллект (ЖИ) қазіргі киберқауіптерді анықтау мен алдын алу саласында шешуші рөл атқарады. Cybersecurity Ventures компаниясының мәліметтері бойынша, 2024 жылы ғаламдық киберқылмыс шығындарының 9,5 триллион АҚШ долларына жетуі күтілуде (сурет 1), бұл ЖИ негізіндегі қауіпсіздік шараларының өзектілігін көрсетеді [Morgan S., Calif S., 2024].



Сурет 1. 2020-2024 жылдар аралығындағы ғаламдық киберқылмыс шығындарының өсуі

McKinsey компаниясының 2024 жылдың басындағы зерттеуіне сәйкес, ұйымдардың 65% өздерінің бизнес функцияларында ЖИ-ді тұрақты түрде қолданатынын хабарлады, бұл өткен жылмен салыстырғанда екі есе көп. Бұл үрдіс киберқауіпсіздік саласына да айтарлықтай әсер етеді [Singla A. et al, 2024].

ЖИ жүйелері кибершабуылдарды анықтап, оларды ертерек болжауға мүмкіндік береді, бұл ақпараттық қауіпсіздік саласындағы ең маңызды аспект болып табылады. ЖИ алгоритмдері арқылы жасалған жүйелер үнемі деректерді талдап, жаңа қауіптер мен шабуылдарды уақытында анықтай алады. Бұл қауіптерді анықтаудың дәлдігі мен жылдамдығы киберқауіпсіздікті күшейтуге және шығындарды азайтуға мүмкіндік береді.

Жалпы алғанда, бұл деректер ЖИ технологияларының киберқауіптерді тиімді басқаруға қабілеттілігін және олардың киберқауіпсіздік саласындағы маңызды рөлін айқындайды. Қауіптер мен тәуекелдер үздіксіз өзгеріп отырғандықтан, ЖИ жүйелерінің үнемі жетілдіріліп отыруы қажет. Тек осылай ғана киберқұқықбұзушылықтарды дер кезінде анықтап, алдын алуға болады.

Пікір алмасу

Жасанды интеллекттің (ЖИ) киберқауіпсіздік саласындағы әлеуеті зор. ЖИ негізіндегі жүйелер қауіптерді анықтау мен алдын алу әдістерін жетілдіруге көмектесіп, машиналық оқыту және тереңдетілген оқыту алгоритмдерін қолдану арқылы үлкен көлемдегі деректерді нақты уақыт режимінде талдауға мүмкіндік береді [Muheidat F. et al. 2024]. Бұл тәсіл ұйымдарға күрделі кибершабуылдарды ертерек анықтауға және оларды тиімді түрде болдырмауға көмектеседі.

ЖИ шешімдері инциденттерге жауап беру уақытын қысқартып, шабуылдан келетін шығындарды азайтуда маңызды рөл атқарады. Сонымен қатар, мінез-құлықтық аналитика әдістері қолданушылардың іс-әрекеттерін қадағалап, күдікті белсенділікті алдын ала

анықтауға мүмкіндік береді. Adversarial AI технологиялары жаңа пайда болған қауіптермен күресуде маңызды құралға айналуда. ЖИ негізіндегі қауіптер туралы барлау платформалары қауіптерді анықтау мен қауіпсіздік шараларын оңтайландыруды жылдамдатып, ұйымдардың қорғаныс мүмкіндіктерін жақсартады [Muheidat F. et al., 2024].

Дегенмен, ЖИ жүйелерінің қауіпсіздігін қамтамасыз ету өзекті мәселелердің бірі болып табылады. ЖИ алгоритмдерінде осалдықтар болуы мүмкін, бұл оларды хакерлер үшін осал нысанаға айналдырады. Мысалы, кейбір ЖИ алгоритмдері қате деректерді өңдеу немесе үлгілерді дұрыс танымай қалу салдарынан шабуылдарға ұшырауы мүмкін. Сондықтан, ЖИ жүйелерін үздіксіз бақылап, қауіпсіздігін үнемі жаңартып отыру қажет.

Тағы бір маңызды аспект – ЖИ шешімдерін енгізуге кететін жоғары шығындар. Мұндай жүйелерді тиімді пайдалану үшін жоғары деңгейдегі техникалық инфрақұрылым мен білікті мамандар қажет. Сонымен қатар, үлкен көлемдегі деректерді жинау және өңдеу қажеттілігі де қосымша шығындарды талап етеді. Дегенмен, ұзақ мерзімді перспективада ЖИ технологияларын қолдану ұйымдардың шығындарын оңтайландырып, экономикалық тиімділікті арттыруға мүмкіндік береді.

Киберқауіпсіздік саласындағы болашақ трендтер ЖИ-дің әртүрлі әдістерді біріктіріп қолдануымен байланысты. Гибридті тәсілдер, яғни машиналық оқыту, ережеге негізделген жүйелер, сараптамалық білім және ойын теориялық модельдері арқылы кешенді шешімдер әзірлеу жоспарлануда [Muheidat F. et al., 2024].

Федеративті және бөлінген оқыту технологиялары бірнеше ұйым немесе құрылғы арасында бірлесіп модель дайындауға мүмкіндік береді. Бұл деректер құпиялылығын сақтай отырып, ЖИ моделін кең көлемде масштабтауға жағдай жасайды. Автоматтандырылған ерекшелік инженериясы мен толық циклды оңтайландыру модельді баптау процесін тиімді етіп, адам факторына тәуелділікті азайтады.

Болашақта reinforcement learning және active learning әдістері ЖИ жүйелерінің үздіксіз өзін-өзі жетілдіруіне мүмкіндік береді, бұл киберқауіпсіздік саласындағы тұрақты қорғанысты қамтамасыз етеді. Сонымен қатар, ЖИ технологияларын блокчейн, кванттық есептеулер, шеткі есептеу сияқты алдыңғы қатарлы инновациялармен біріктіру қауіпсіздік, масштабталу және жүйенің төзімділігін арттыруға көмектеседі.

Қорытынды

Жасанды интеллект технологияларының киберқауіптерді анықтау мен алдын алудағы рөлі қазіргі ақпараттық қауіпсіздік саласында маңызды орын алуда. Жасанды интеллекттің деректерді жылдам өңдеу, үлкен көлемдегі ақпаратты талдау және нақты уақыт режимінде шешім қабылдау қабілеті киберқауіпсіздік жүйелеріне жаңа мүмкіндіктер ашады. Машиналық оқыту, үлгілерді тану және болжамды модельдер сияқты әдістер зиянды бағдарламалар мен әрекеттерді ерте кезеңде анықтап, олардың салдарын болдырмауға мүмкіндік береді. Сонымен қатар, жасанды интеллекттің бейімделу және өзін-өзі жетілдіру мүмкіндіктері заманауи қауіп-қатерлерге жауап беру үшін аса маңызды рөл атқарады. Ол шабуылдардың өзгермелі сипаттамаларын бақылап, жаңа әдістерге бейімделе алады, бұл өз кезегінде киберқауіпсіздік жүйелерінің тиімділігін арттырады.

Алайда, жасанды интеллектті енгізуде кейбір қиындықтар мен шектеулер де кездеседі. Жасанды интеллекттің мүмкіндіктері киберқауіпсіздікті күшейтсе де, адамдар бұл технологияны өз пайдасына пайдалануы мүмкін, соның нәтижесінде жаңа қауіптер пайда болады. Әсіресе, жасанды интеллектке негізделген жүйелердің қауіпсіздігін қамтамасыз ету, этикалық нормаларды сақтау және оның дұрыс қолданылуын бақылау аса маңызды мәселелер болып табылады. Сондай-ақ, жасанды интеллект киберқауіптерді болжау және жоюда тиімді құрал болғанымен, оның қолдану шығындары, техникалық күрделілігі және дұрыс басқарылмауы жаңа қатерлерді тудыруы мүмкін. Осыған байланысты, бұл технологияны

дамыту барысында кешенді зерттеулер жүргізу және тәжірибеде қолдану әдістерін жетілдіру қажет.

Жалпы алғанда, жасанды интеллекттің киберқауіпсіздік саласындағы рөлі болашақта ақпараттық қауіпсіздікті қамтамасыз етуде негізгі құралға айналатыны сөзсіз. Жасанды интеллектті кеңінен қолдану кибершабуылдар қаупін азайтып, ақпараттық инфрақұрылымдардың тұрақтылығын арттыруға мүмкіндік береді. Бұл технологияның дамуы қоғамдағы ақпараттық жүйелерді қорғауда маңызды рөл атқарып, киберқауіптермен күресте үлкен үлес қосатыны анық.

Пайдаланылған әдебиеттер тізімі

Chen H., Wang F.Y. (2005) Guest Editors' Introduction: Artificial Intelligence for Homeland Security. *IEEE Intelligent Systems*, 20, 5, 12-16. DOI: https://doi.org/10.1109/MIS.2005.88 (өтінім берілген күні: 14.12.2024).

Stytz M.R., Lichtblau D.E., Banks S.B. (2005) Toward using intelligent agents to detect, assess, and counter cyberattacks in a network-centric environment, *Ft. Belvoir Defense Technical Information Center*, 1, Edition, Alexandria, VA [Электрондық ресурс]: URL: https://www.researchgate.net/publication/228845360_Toward_using_intelligent_agents_to_detect_assess_and_counter_cyberattacks_in_a_network-centric_environment (өтінім берілген күні: 09.01.2025).

Helano J., Nogueira M. (2006) Mobile Intelligent Agents to Fight Cyber Intrusions. *The International Journal of Forensic Computer Science (IJoFCS)*, 1, 28-32 [Электрондық ресурс]: URL: https://www.researchgate.net/publication/267718557_Mobile_Intelligent_Agents_to_Fight_Cyber_Intrusions (өтінім берілген күні: 17.12.2024).

Dasgupta D. (2006) Computational Intelligence in Cyber Security. *IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety* (CIHSPS 2006), 2-3. DOI: https://doi.orh/10.1109/CIHSPS.2006.313289 (өтінім берілген күні: 22.12.2024).

Perols R., Murthy U. (2018) The Impact of Cybersecurity Risk Management Examinations and Cybersecurity Incidents on Investor Perceptions. *SSRN Electronic Journal.* DOI: https://doi.org/10.2308/AJPT-18-010 (өтінім берілген күні: 06.01.2025).

Mengidis N., Tsikrika T., Vrochidis S., Kompatsiaris I. (2019) Blockchain and AI for the Next Generation Energy Grids: *Cybersecurity Challenges and Opportunities, Information & Security: An International Journal*, 43(1), 21-33. DOI: https://doi.org/10.11610/isij.4302 (өтінім берілген күні: 24.12.2024).

Chung S. (2021) AI-Based Cybersecurity: Benefits and Limitations. *AI Journal*, 1-2. DOI: https://doi.org/10.22471/ai.2021.6.1.18 (өтінім берілген күні: 29.12.2024).

Тастанбеков М.Б., Омаров Б.С. (2024) *Машиналық оқыту арқылы қаржылық алаяқтықты анықтаудың әдістері.* DOI: https://doi.org/10.5281/zenodo.14498352 (өтінім берілген күні: 11.01.2025).

Ansari M., Dash B., Sharma P., Yathiraju N. (2022) The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. *International Journal of-Advances Research in Computer and Communication Engineering*, 11, 9, September, 81-90. DOI: https://doi.org/10.17148/IJARCCE.2022.11912 (өтінім берілген күні: 05.02.2025).

Shafqat N. (2016) Comparative Analysis of Various National Cyber Security Strategies. *International Journal of Computer Science and Information Security (IJCSIS)*, 136 [Электрондық ресурс]: URL: https://www.academia.edu/21451805/Comparative_Analysis_of_Various_National_Cyber_Security_Strategies (өтінім берілген күні: 19.12.2024).

Solms R., Niekerk J. (2013) *From information security to cyber security*. DOI: https://doi.org/10.1016/j.cose.2013.04.004 (өтінім берілген күні: 02.01.2025).

Ghelani D. (2022) Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. *American Journal of Science, Engineering and Technology*, September 22. DOI: https://doi.org/10.22541/au.166385207.73483369/v1 (өтінім берілген күні: 08.12.2024).

Ghate S., Agrawal P.K. (2017) A Literature Review on Cyber Security in Indian Context. *Journal of*

Computer Information Technology, 8(5), 30-36 [Электрондық ресурс]: URL: https://pdfs.semanticscholar.org/952f/ddfcc397fc565cf0c63ffcf590b402d3b24a.pdf (өтінім берілген күні: 27.12.2024).

Abrahams T.O., Ewuga S.K., Kaggwa S., Uwaoma P.U., Hassan A.O., Dawodu S.O. (2024) Mastering Compliance: A Comprehensive Review of regulatory frameworks in accounting and cybersecurity. *Computer Science & IT Research Journal*, 5, 1, 120-140. DOI: https://doi.org/10.51594/csitrj.v5i1.709 (өтінім берілген күні: 31.01.2025).

Kumar S., Kumar H., Gunnam G.R. (2019) Security Integrity of Data Collection from Smart Electric Meter under a Cyber Attack, *2nd International Conference on Data Intelligence and Security (ICDIS)*, South Padre Island, TX, USA, 9-13. DOI: https://doi.org/10.1109/ICDIS.2019.00009 (өтінім берілген күні: 15.01.2025).

Kanade V. (2022) What is Machine Learning? Definition, Types, Applications, and Trends. *Spiceworks* [Электрондық ресурс]: URL: https://www.spiceworks.com/tech/artificialintelligence/articles/what-is-ml/ (өтінім берілген күні: 07.12.2024).

Morgan S., Calif S. (2024) 2024 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics. *Cybercrime*, June 24 [Электрондық ресурс]: URL: https://cybersecurityventures.com/cybersecurity-almanac-2024/ (өтінім берілген күні: 04.02.2025).

Singla A., Sukharevsky A., Yee L., Chui M., Hall B. (2024) *The State of AI in Early 2024: Gen AI Adoption Spikes and Starts to Generate Value.* McKinsey & Company, 23 [Электрондық ресурс]: URL: https://www.mckinsey.com/~/media/mckinsey/business%20functions/quantumblack/our%20insights/the%20state%20of%20ai/2024/the-state-of-ai-in-early-2024-final.pdf (өтінім берілген күні: 08.02.2025).

Muheidat F., Mallouh M. A., Al-Saleh O., Al-Khasawneh O., Tawalbeh L.A. (2024) Applying AI and Machine Learning to Enhance Automated Cybersecurity and Network Threat Identification. *Procedia Computer Science,* 251, 287-294. DOI: https://doi.org/10.1016/j.procs.2024.11.112 (өтінім берілген күні: 21.01.2025).

References

Chen H., Wang F.Y. (2005) Guest Editors' Introduction: Artificial Intelligence for Homeland Security. *IEEE Intelligent Systems,* 20, 5, 12-16. DOI: https://doi.org/10.1109/MIS.2005.88 (otinim berilgen kuni: 14.12.2024).

Stytz M.R., Lichtblau D.E., Banks S.B. (2005) Toward using intelligent agents to detect, assess, and counter cyberattacks in a network-centric environment, *Ft. Belvoir Defense Technical Information Center,* 1, Edition, Alexandria, VA [Elektrondyk resurs]: URL: https://www.researchgate.net/publication/228845360_Toward_using_intelligent_agents_to_detect_assess_and_counter_cyberattacks_in_a_network-centric_environment (otinim berilgen kuni: 09.01.2025).

Helano J., Nogueira M. (2006) Mobile Intelligent Agents to Fight Cyber Intrusions. *The International Journal of Forensic Computer Science (IJoFCS),* 1, 28-32 [Elektrondyk resurs]: URL: https://www.researchgate.net/publication/267718557_Mobile_Intelligent_Agents_to_Fight_Cyber_Intrusions (otinim berilgen kuni: 17.12.2024).

Dasgupta D. (2006) Computational Intelligence in Cyber Security. *IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety (CIHSPS 2006),* 2-3. DOI: https://doi.orh/10.1109/CIHSPS.2006.313289 (otinim berilgen kuni: 22.12.2024).

Perols R., Murthy U. (2018) The Impact of Cybersecurity Risk Management Examinations and Cybersecurity Incidents on Investor Perceptions. *SSRN Electronic Journal*. DOI: https://doi.org/10.2308/AJPT-18-010 (otinim berilgen kuni: 06.01.2025).

Mengidis N., Tsikrika T., Vrochidis S., Kompatsiaris I. (2019) Blockchain and AI for the Next Generation Energy Grids: *Cybersecurity Challenges and Opportunities, Information & Security: An International Journal,* 43(1), 21-33. DOI: https://doi.org/10.11610/isij.4302 (otinim berilgen kuni: 24.12.2024).

Chung S. (2021) AI-Based Cybersecurity: Benefits and Limitations. *AI Journal,* 1-2. DOI: https://doi.org/10.22471/ai.2021.6.1.18 (otinim berilgen kuni: 29.12.2024).

Tastanbekov M.B., Omarov B.S. (2024) *Mashinalyk okytu arkyly karzhylyk alayaktykty anyktaudyn adisteri.* DOI: https://doi.org/10.5281/zenodo.14498352 (otinim berilgen kuni: 11.01.2025).

Ansari M., Dash B., Sharma P., Yathiraju N. (2022) The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. *International Journal of-Advances Research in Computer and Communication Engineering,* 11, 9, September, 81-90. DOI: https://doi.org/10.17148/IJARCCE.2022.11912 (otinim berilgen kuni: 05.02.2025).

Shafqat N. (2016) Comparative Analysis of Various National Cyber Security Strategies. *International Journal of Computer Science and Information Security (IJCSIS),* 136 [Elektrondyk resurs]: URL: https://www.academia.edu/21451805/Comparative_Analysis_of_Various_National_Cyber_Security_Strategies (otinim berilgen kuni: 19.12.2024).

Solms R., Niekerk J. (2013) *From information security to cyber security.* DOI: https://doi.org/10.1016/j.cose.2013.04.004 (otinim berilgen kuni: 02.01.2025).

Ghelani D. (2022) Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. *American Journal of Science, Engineering and Technology,* September 22. DOI: https://doi.org/10.22541/au.166385207.73483369/v1 (otinim berilgen kuni: 08.12.2024).

Ghate S., Agrawal P.K. (2017) A Literature Review on Cyber Security in Indian Context. *Journal of Computer Information Technology,* 8(5), 30-36 [Elektrondyk resurs]: URL: https://pdfs.semanticscholar.org/952f/ddfcc397fc565cf0c63ffcf590b402d3b24a.pdf (otinim berilgen kuni: 27.12.2024).

Abrahams T.O., Ewuga S.K., Kaggwa S., Uwaoma P.U., Hassan A.O., Dawodu S.O. (2024) Mastering Compliance: A Comprehensive Review of regulatory frameworks in accounting and cybersecurity. *Computer Science & IT Research Journal,* 5, 1, 120-140. DOI: https://doi.org/10.51594/csitrj.v5i1.709 (otinim berilgen kuni: 31.01.2025).

Kumar S., Kumar H., Gunnam G.R. (2019) Security Integrity of Data Collection from Smart Electric Meter under a Cyber Attack, *2nd International Conference on Data Intelligence and Security (ICDIS),* South Padre Island, TX, USA, 9-13. DOI: https://doi.org/10.1109/ICDIS.2019.00009 (otinim berilgen kuni: 15.01.2025).

Kanade V. (2022) What is Machine Learning? Definition, Types, Applications, and Trends. *Spiceworks* [Elektrondyk resurs]: URL: https://www.spiceworks.com/tech/artificialintelligence/articles/what-is-ml/ (otinim berilgen kuni: 07.12.2024).

Morgan S., Calif S. (2024) 2024 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics. *Cybercrime,* June 24 [Elektrondyk resurs]: URL: https://cybersecurityventures.com/cybersecurity-almanac-2024/ (otinim berilgen kuni: 04.02.2025).

Singla A., Sukharevsky A., Yee L., Chui M., Hall B. (2024) *The State of AI in Early 2024: Gen AI Adoption Spikes and Starts to Generate Value.* McKinsey & Company, 23 [Elektrondyk resurs]: URL: https://www.mckinsey.com/~/media/mckinsey/business%20functions/quantumblack/our%20insights/the%20state%20of%20ai/2024/the-state-of-ai-in-early-2024-final.pdf (otinim berilgen kuni: 08.02.2025).

Muheidat F., Mallouh M. A., Al-Saleh O., Al-Khasawneh O., Tawalbeh L.A. (2024) Applying AI and Machine Learning to Enhance Automated Cybersecurity and Network Threat Identification. *Procedia Computer Science,* 251, 287-294. DOI: https://doi.org/10.1016/j.procs.2024.11.112 (otinim berilgen kuni: 21.01.2025).

Использование искусственного интеллекта для выявления и предотвращения киберугроз

[1]Д.Нсанбаев, [1]Ш.К.Ележанова
[1]Атырауский университет имени Х.Досмухамедова (Атырау, Казахстан)

Аннотация
В статье рассматривается использование технологий искусственного интеллекта (ИИ) для выявления и предотвращения киберугроз. С развитием цифровой эпохи увеличивается количество и сложность кибератак. Традиционные методы часто оказываются недостаточно эффективными в борьбе с этими угрозами, что подчеркивает необходимость внедрения современных подходов. Технологии ИИ

позволяют вывести кибербезопасность на новый уровень благодаря быстрой обработке больших объемов данных, выявлению аномалий и проактивному реагированию на атаки. Основная цель статьи - оценить эффективность применения технологий ИИ и предложить пути их интеграции в современные системы кибербезопасности. В ходе исследования использовались алгоритмы машинного обучения и методы обработки данных для анализа точности и скорости обнаружения атак. Результаты показали высокую эффективность ИИ-инструментов по сравнению с традиционными методами. Данная работа вносит вклад в исследования в области кибербезопасности и нацелена на открытие новых возможностей для защиты информационной инфраструктуры. Кроме того, в статье обсуждаются возможные трудности внедрения этих методов и пути их решения.
Ключевые слова: киберугрозы, искусственный интеллект, анализ данных, машинное обучение, выявление аномалий, информационная безопасность.

Using Artificial Intelligence for detecting and preventing cyber threats

[1]D.Nsanbaev, [1]Sh.K.Yelezhanova
[1]Kh.Dosmukhamedov Atyrau University (Atyrau, Kazakhstan)

Abstract
This article explores the use of artificial intelligence (AI) technologies for detecting and preventing cyber threats. With the advancement of the digital age, the number and complexity of cyberattacks are increasing. Traditional methods often fall short in countering these threats, highlighting the need for modern approaches. AI technologies enable cybersecurity to reach a new level by rapidly processing large volumes of data, detecting anomalies, and proactively responding to attacks. The main objective of the article is to evaluate the effectiveness of AI technologies and propose ways to integrate them into modern cybersecurity systems. The study utilized machine learning algorithms and data processing methods to analyze their accuracy and speed in detecting attacks. The findings demonstrated the superior efficiency of AI tools compared to traditional methods. This work contributes to research in the field of cybersecurity and aims to unlock new opportunities for protecting informational infrastructure. Additionally, the article discusses potential challenges in implementing these methods and solutions to address them.
Keywords: cyber threats, artificial intelligence, data analysis, machine learning, anomaly detection, information security.

Поступила в редакцию: 21.01.2025
Одобрена: 19.03.2025
Первая публикация на сайте: 13.08.2025

МРНТИ: 87.13.29 https://doi.org/10.65247/3105-3432-2025-4.04

DYNAMICS OF CHANGES IN THE COASTLINE OF THE NORTHERN CASPIAN SEA FOR THE PERIOD 2016-2024

*[1]S.JARAS, *[1]A.Ye.YEGINBAYEVA*
[1]L.N.Gumilyov Eurasian National University
(Astana, Kazakhstan),
*[1]zsajaly@gmail.com, *[1]yeginbayeva_aye@enu.kz*

Abstract
The article examines the dynamics of coastline changes in the Northern Caspian Sea from 2016 to 2024 based on remote sensing and cartographic data. It identifies key transformation directions, highlighting areas of active erosion and accretion. The study considers natural and anthropogenic factors influencing these changes, including fluctuations in sea level, climatic conditions, and economic activities. The results help assess the environmental and socio-economic consequences of coastal zone transformation. Additionally, the study provides recommendations to mitigate negative impacts on the Northern Caspian Sea ecosystem, aiming to balance environmental sustainability with human activities in the region. The findings contribute to better coastal management and long-term ecological preservation.