ҒТАМР 14.35.09 https://doi.org/10.26577/JES20247801015

М. Серік[1*], Д.Ш. Тлеумагамбетова[1], С.Ғ. Құрымбаев[2], Г.Е. Самашова[3]

[1]Л.Н. Гумилев атындағы Еуразия Ұлттық университеті, Қазақстан, Астана қ.
[3]Е.А. Бөкетов атындағы Қарағанды университеті, Қазақстан, Қарағанды қ.
[4]Абылқас Сағынов атындағы Қарағанды техникалық университеті, Қазақстан, Қарағанды қ.
*e-mail: serik_meruerts@mail.ru

«АҚПАРАТТЫҚ ҚАУІПСІЗДІК» АРНАЙЫ КУРСЫНЫҢ МАЗМҰНЫН ОҚУ ПРОЦЕСІНДЕ ЖЕТІЛДІРУ: МАШИНАЛЫҚ ОҚЫТУДЫҢ КӨМЕГІМЕН КИБЕРШАБУЫЛДАРДЫ АНЫҚТАУ

Қазіргі таңда ақпараттық-коммуникациялық технологиялардың дамуы нәтижесінде ақпараттық шабуылдарды қолданыстағы дәстүрлі әдіс-тәсілдермен анықтау тиімсіз болуы фактілері анықталуда. Ал, машиналық оқыту алгоритмдері интернет протоколының трафигін жіктеу, шабуылдарды анықтау үшін дұрыс емес трафикті сүзуден бастап тривиальды шабуылдарға жауап беру сияқты мәселелерді шешудің тиімді шешімін табуда. Сондықтан біздің зерттеу жұмысымызда Л.Н.Гумилев атындағы Еуразия ұлттық университетінің «6В01511-Информатика» білім беру бағдарламасының ақпараттық қауіпсіздікке байланысты арнайы курсының мазмұнын заманауи ақпараттық технологиялардың дамуына сәйкес жетілдіру негізге алынды. Сәйкесінше, зерттеу жұмысының мақсаты – нейронды желілердің көмегімен кибершабуылдарды анықтау мен жоғары оқу орнының білім мазмұнына ендіру. Зерттеу жұмысының мақсатына сәйкес кибершабуылдары бар деректерді жинақтау, деректерді кластарға жіктеу, нейронды желі моделін әзірлеу, әзірленген модель негізінде кибершабуылдарды анықтау сияқты жұмыстар атқарылды. Әзірленген модельді кез-келген салада қандай да бір процесті анықтау үшін қолдануға болады. Зерттеу жұмысының нәтижесі бойынша сауалнама қорытындысы білім алушылардың арнайы курс мазмұнына қанағаттану деңгейінің 55%-ға артқандығын байқаймыз. Демек, ақпараттық қауіпсіздік саласы бойынша білім беру мазмұнын жетілдіру оң нәтиже берді. Болашақта жаңартылған арнайы курсты еліміздің жетекші жоғары оқу орнына қолжетімді болатындай жүзеге асырылады.

Түйін сөздер: нейронды желілер, кибершабуыл, машиналық оқыту, білім беру жүйесі, көпқабатты персептрон.

M. Serik[1*], D. Tleumagambetova[1], S. Kurymbayev[2], G. Samashova[3]

[1]L.N. Gumilyov Eurasian National University, Kazakhstan, Astana
[2]Buketov Karagandy University, Kazakhstan, Karaganda
[3]A. Saginov Karaganda Technical University, Kazakhstan, Karaganda
*e-mail: serik_meruerts@mail.ru

Improving the content of the special course “Information Security” during the training process: detecting cyber attacks using machine learning

Currently, as a result of the development of information and communication technologies, facts are being revealed that the detection of information attacks using existing traditional methods is ineffective. Meanwhile, machine learning algorithms find effective solutions to problems such as classifying Internet Protocol traffic, filtering malformed traffic to detect attacks, and responding to trivial attacks. Therefore, our research work was based on improving the content of a special course on information security of the educational program «6B01511-Informatics» of the L. N.Gumilyov Eurasian National University in accordance with the development of modern information technologies. Accordingly, the goal of the research work is to identify cyber-attacks using neural networks. In accordance with the purpose of the research work, work was carried out such as collecting data with cyber-attacks, classifying data into classes, developing a neural network model, identifying cyber-attacks based on the developed model. The developed model can be used to define any process in any area. According to the survey results, we see that the level of student satisfaction with the content of the special course increased by 55%. Thus, improving the content of education in the field of information security has yielded positive results. In the future, the updated special course will be available to the country’s leading higher education institutions.

Key words: neural networks, cyber-attack, machine learning, educational system, multilayer perceptron.

М. Серик[1*], Д.Ш. Тлеумагамбетова[1], С.Г. Курымбаев[2], Г.Е. Самашова[3]
[1]Евразийский национальный университет имени Л.Н. Гумилева, Казахстан, г. Астана
[2]Карагандинский университет имени Е.А. Букетова, Казахстан, г. Караганда
[3]Карагандинский технический университет имени А. Сагинова, Казахстан, г. Караганда
*e-mail: serik_meruerts@mail.ru

Совершенствование содержания специального курса «Информационная безопасность» в процессе обучения: выявление кибератак с использованием машинного обучения

В настоящее время в результате развития информационно-коммуникационных технологий выявляются факты неэффективности выявления информационных атак существующими традиционными методами. Тем временем алгоритмы машинного обучения находят эффективные решения таких проблем, как классификация трафика интернет-протокола, фильтрация искаженного трафика для обнаружения атак и реагирование на тривиальные атаки. Поэтому в нашей исследовательской работе за основу было взято совершенствование содержания специального курса по информационной безопасности образовательной программы «6В01511-Информатика» Евразийского национального университета им.Л.Н. Гумилева в соответствии с развитием современных информационных технологий. Соответственно, целью исследовательской работы является выявление кибератак с использованием нейронных сетей. В соответствии с целью исследовательской работы были проведены такие работы, как сбор данных с кибератаками, классификация данных по классам, разработка модели нейронной сети, выявление кибератак на основе разработанной модели. Разработанная модель может быть использована для определения любого процесса в любой области. По результатам опроса мы видим, что уровень удовлетворенности студентов содержанием спецкурса увеличился на 55%. Таким образом, совершенствование содержания образования в области информационной безопасности дало положительные результаты. В дальнейшем обновленный спецкурс будет доступен ведущим высшим учебным заведениям страны.

Ключевые слова: нейронные сети, кибератака, машинное обучение, образовательная система, многослойный перцептрон.

Кіріспе

Қазіргі әлем күнделікті өмірдің барлық аспектілерінің киберкеңістікке толығымен тәуелді болуына байланысты оны пайдалану жағдайлары күн сайын артып келеді. Интернет желісінде киберқауіптер мен киберқылмыстардың артуына байланысты оларды қалыпты антивирустық немесе ақпараттың қауіпсіздік құралдарымен төтеп беру мүмкін емес болатындай жағдайлары тіркелуде. Киберқылмыскерлер уақыт өте келе қорғаныс қабырғасын жеңу үшін әдістерін өзгертеді. Кәдімгі әдістер күндік шабуылдар мен күрделі шабуылдарды анықтай алмайды. Осы уақытқа дейін киберқылмыстарды анықтау және киберқауіптермен күресу үшін көптеген машиналық оқыту әдістері әзірленді. Бұл зерттеу жұмысының мақсаты – машиналық оқытудың саласы нейронды желілердің көмегімен кибершабуылдарды анықтау.

Зерттеу тақырыбы аясында Қазақстан Республикасы Ғылым және жоғары білім министрлігі тарапынан гранттық қаржыландыру негізінде AP19677348 «Білімнің жаһандануы жағдайында жасанды интеллектің бағыты машиналық оқыту негізінде информатика мұғалімдерінің даярлықтарын жетілдіруге арналған ақпараттық білім порталын құру» атты ғылыми жобасы жүзеге асырылуда. Бұл ақпараттық білім порталы машиналық оқыту, ақпараттық қауіпсіздік, бұлтты технологиялар, үлкен деректер сияқты бөлімдерді де қамтиды. Жалпы ақпараттық қауіпсіздік машиналық оқытудың бақыланатын оқыту және бақыланбайтын оқытудың барлық жағдайларында қолданылады (Dasgupta, 2022: 106) [1].

Киберқауіпсіздік саласындағы бақыланатын машиналық оқыту деректерді жіктеу немесе нәтижелерді болжау үшін қолданылады. Ол алгоритмдерді үйрету және көрсетілген кіріс және шығыс деректерімен корреляцияға бағаланатын айнымалыларды анықтау үшін белгіленген деректер жиынтығын пайдаланады. Киберқауіпсіздік саласындағы бақыланатын машиналық оқыту бірнеше тәсілдермен қолданылады, соның ішінде: сканерлеу және ауыстыру сияқты желілік тәуекелдердің бірегей белгілерін анықтау, белгілі бір қауіпсіздік қаупі үшін мақсатты айнымалыны болжау немесе жіктеу (мысалы, таратылған қызмет көрсетуден бас тарту немесе DDOS-Distributed Denial of Service шабуылы), жаңа үлгілердің зиянды екенін болжауға көмектесу үшін қатерсіз және зиянды үлгілердегі оқу үлгілері.

Киберқауіпсіздіктегі бақыланбайтын машиналық оқыту таңбаланбаған деректер жиынтығын (мысалы, фотосуреттер, аудио және бейне жазбалар, мақалалар немесе әлеуметтік медиа жазбалары) талдау және кластерлеу үшін қолданылады. Ол адамның араласуынсыз жасырын заңдылықтарды немесе деректерді топтастыруды анықтай алады. Алгоритм ақпаратты ішкі жиындарға топтастыру үшін қолданылатын үлгілерді іздеуде деректер жиындарын қарайды. Бақыланбайтын машиналық оқыту көбінесе терең оқыту үшін қолданылады. Киберқауіпсіздік саласындағы бақыланбайтын машиналық оқытуды бірнеше жолмен қолдануға болады, соның ішінде: ерекше мінез-құлықты анықтау, шабуылдардың жаңа үлгілерін анықтау, күндік шабуылдарды азайту.

Сонымен қатар, жартылай басқарылатын киберқауіпсіздік машиналарын оқыту бақыланатын және бақыланбайтын машиналық оқытуды біріктіреді. Ол бақыланатын оқыту алгоритмі үшін таңбаланған деректер жеткіліксіз болған кезде белгілерді жіктеу және алу үшін үлкенірек таңбаланбаған деректер жиынтығынан шағын таңбаланған деректер жинағын шығарады. Ол сондай-ақ, деректер жиынтығын таңбалау өте қымбат болған кезде қолданылады. Киберқауіпсіздікті қамтамасыз ету үшін ішінара бақыланатын машиналық оқытуды мыналар үшін пайдалануға болады: қарсылас нейрондық желілер, зиянды және қатерсіз боттарды анықтау, зиянды программаны анықтау, төлем программаларын анықтау. Осындай типті ақпараттық қауіпсіздік мәселелері біздің зерттеу жұмысымызда қарастырылады.

Әдебиеттерге шолу

Ақпараттық қауіпсіздік шараларын машиналық оқыту алгоритмдері көмегімен көптеген отандық, шетелдік ғылыми зерттеуші практиктер өздерінің ғылыми жұмыстарында қарастырды. Атап айтқанда, G.Apruzzese пен P.Laskov-тың «Машиналық оқытудың киберқауіпсіздіктегі ролі» зерттеу жұмысында машиналық оқытудың ақпараттық қауіпсіздік саласына қалай әсер ететінін және нақты қай бағытта қолдануға болатындығы көрсетілген (Apruzzese, 2022:33) [2]. Galina Momcheva, Ali Sabra «Machine learning in cybersecurity» кітабында ақпараттық қауіпсіздіктің негізгі аспектілерінде фишинг, кредит карта, Интернет заттар, зиянды программалардағы қауіп-қатерлерді машиналық оқыту алгоритмдерімен алдын-алу шаралары қарастырылған (Momcheva, 2022: 69) [3]. Сонымен қатар, M. A. Manjramkar пен K. C. Jondhalenің «Cyber Security Using Machine Learning Techniques» еңбегінде ақпараттық қауіпсіздік саласында машиналық оқыту технологияларының маңыздылығы мен нақты қай алгоритмдерді қолдану қажеттігі қарастырылған (Manjramkar, 2022:701) [4]. Дәл сол сияқты P. Kantamsetti-дің «Machine learning applications in the field of cyber security» атты жұмысында ұйымда фишингтік сілтемелердің болуын анықтау, желілік трафикті бақылау, активтер мен хаттамалардың қауіпсіздігін тексеру, спамды анықтау және киберкеңістіктегі күнделікті жұмысты аутоматтандыру мәселелері қарастырылады (Kantamsetti, 2021:103) [5]. Сонымен қатар, ақпараттық қауіпсіздік саласында машиналық оқытуды қолдануды жетік меңгеру мақсатында Bharadiya J.P.-ның «Machine Learning in Cybersecurity: Techniques and Challenges» еңбегі қарастырылды. Мақалада автор киберқауіпсіздік саласындағы машиналық оқытудың бірнеше қосымшаларын қарастырған, яғни фишингті анықтау, желіге кіруді анықтау, пернелерді басу динамикасының аутентификациясы, криптография, адамдардың өзара әрекеттесуінің дәлелі, әлеуметтік желілердегі спамды анықтау, смарт есептегіштердің энергия тұтынуын профильдеу және машиналық оқыту әдістеріне қатысты қауіпсіздік мәселелері осы зерттеуде қамтылған. Машиналық оқыту модельдері фишингтік хаттар мен веб-сайттарды жоғары дәлдікпен және жалған позитивтердің төмен деңгейімен тиімді анықтай алатындығы нақты мысалдармен келтірілген. Фишингті анықтауды жақсарту үшін фишингтің жаңа әдістерін қосу үшін оқу деректер жинағын үздіксіз жаңартып отыру және өнімділікті жақсарту үшін машиналық оқытудың бірнеше үлгілерін біріктіретін ансамбльдік әдістерді қолдану ұсынылатыны туралы қарастырылған(Bharadiya, 2023:14) [6]. Дәл сол сияқты, ақпараттық қауіпсіздік саласында машиналық оқытудың жағдайын түсіну үшін Suresh P-ның «Contemporary survey on effectiveness of machine and deep learning techniques for cyber security» мақаласы қарастырылды. Автор сәйкестендіру, модельдеу, қадағалау және талдау сияқты киберқауіпсіздік мақсаттарын ілгерілету, сондай-ақ құпия деректер мен қауіпсіздік жүйелеріне төнетін әртүрлі қауіптерден қорғау үшін машиналық және терең оқыту тәсілдерін қалай пайдалануға болатынын

қарастырған. Мақаладағы мысалдарда әртүрлі киберқауіпсіздік мәселелерін машиналық оқыту және терең оқыту жағдайы келтірілген(Suresh, 2022: 200) [7]. Shaukat K.-ның «A Survey on Machine Learning Techniques for Cyber Security in the Last Decade» атты мақаласында соңғы онжылдықта компьютерлік желілер мен мобильді желілердегі интрузияларды, спамдарды анықтауды және зиянды бағдарламаларды анықтауды қоса алғанда, киберқауіпсіздікке арналған машиналық оқыту әдістері туралы әдебиеттерді ұсына отырып, киберкеңістікті шабуылдардан қорғауда машиналық оқыту әдістерінің алдында тұрған қиындықтарға жан-жақты шолу жасалған. Сондай-ақ, әрбір машиналық оқыту әдісінің қысқаша сипаттамаларын, жиі қолданылатын қауіпсіздік деректер жиынын, маңызды машиналық оқыту құралдарын және жіктеу үлгісін бағалау үшін бағалау көрсеткіштерін, киберқауіпсіздік саласындағы машиналық оқытудың қазіргі тенденцияларын ұсынады(Shaukat, 2020: 222354) [8]. Ahsan M.-нің «Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning» атты мақаласында киберқауіпсіздік жүйелері мен қызметтерінде деректерге негізделген интеллектуалды шешім қабылдауды сәтті орындау үшін машиналық оқыту әдістерінің қалай қолданылатыны зерттелген. Сондай-ақ, оның қауіпсіздік оқиғалары туралы түсінік алу және деректерді бағалау тұрғысынан қауіпсіздік деректеріне қалай әсер ететіні туралы пікірталас ұсынылған. Киберқауіпсіздікпен машиналық оқыту саласындағы болашақ зерттеу идеяларының қызығушылығын көрсету үшін қауіпсіздікті талдаудың әртүрлі негізгі мәселелері талқыланды. Шабуылдар дамыған сайын машиналық оқыту әдістері де дамып, бұл саланы өте динамикалық етеді. Кибершабуылдардан болатын зиянды азайту үшін машиналық оқыту бойынша сарапшылардан ғана емес, сонымен қатар оқытудың соңғы деректер жиынтығын ұсынуға жауапты зерттеушілер мен мекемелерден де тұрақты қолдау қажетті айқындалған. Мекемлердегі ақпараттың қауіпсіздігін күшейту мақсатында машиналық оқытудың алгоритмдерімен қоса шифрлеу алгоритмдерінің маңыздылығы да қарастырылады. Атап айтқанда, гомомофрты шифрлеу тәсілдері зерттелген (Ahsan, 2022: 555) [9].

Көпқабатты перцептронның құрылымы, орындалу принципі және оларды жылдам оқытудың әдістері(импульс әдісі, оқыту жылдамдығына айнымалыны қолдану) қарастырылады. Автор көп қабатты перцептрондарды оқыту үшін кері таралу алгоритмін пайдалана отырып, оларды функционалдық жуықтаудан бастап есептеу жүйесінің жүктемесін бағалау немесе полимерленудің химиялық реакцияларының эволюциясын модельдеу сияқты әртүрлі салалардағы болжауға дейінгі қолданбалардың кең ауқымы үшін пайдалануға болады деп тұжырымдаған. Сонымен қатар, автор алгоритмді іске асыру барысында параметрлерді таңдауға және желіні конфигурациялауға байланысты бірқатар практикалық мәселелерді анықтаған(Popescu, 2009) [10]. Көпқабатты перцептрондардың құрылымы туралы Toha S.F. «MLP and Elman Recurrent Neural Network Modelling for the TRMS» атты жұмысында қарастырады. Автор сонымен қатар басқа да көп қабатты перцептронды қарастырады, ал ол MLP көпқабатты перцептронның ерекшеліктерін ажыратуға мүмкіндік береді. Демек, мұндағы қарастырылған көпқабатты перцептрондың бізідң зерттеуімізде қарастырылатын перцептрондардан ең негізгі айырмашылығы бірнеше шығыс қабаттарына ие болуы және екі факторлы аутентификацияның болуымен қарастырылады(Toha, 2009) [11]. Carlson L. «Using Multilayer Perceptrons as means to predict the end-point temperature in an Electric Arc Furnace» еңбегінде машиналық оқыту моделі, көп қабатты перцептрон зерттелген. Бұл жинақта қарастырылған модель басқа модельдерге қарағанда тиімділігімен кез-келген салада қандай да бір болжамды анықтау үшін қолдануға болады. Демек, деректердің негізінде нақты көпқабатты перцептрон модельді әзірленіп, олардың әрқайсысы сәйкес қателік мәндері негізінде бағаланған. Осы модельдердің бесеуі модель жасалғанға дейінгі көптеген қолайсыз болжамдар мен шарттарға қарамастан, белгіленген модельден дәлдік көрсеткіші өте жоғары болды, себебі кіріс айнымалыларының көбірек болуы модельдің жақсы жұмыс істеуіне ықпал ететіні анықталды (Carlson, 2015: 75) [12]. Abu-Doush I. -ң «Enhancing multilayer perceptron neural network using archive-based harris hawks optimizer to predict gold prices» мақаласында көп қабатты перцептронды нейрондық желіні пайдалану мүмкіндіктері қарастырылған. Мақалада зерттелген көп қабатты перцептронды нейронды желіні зерттеу моделі тиімді

жолмен көрсетілген. Ең бастысы, көпқабатты перцептронды нейронды желінің құрылымын, жұмыс істеу принципі жетік қарастырылған (Abu-Doush, 2023) [13].

Зерттеуші ғалымдардың ақпараттық қауіпсіздік саласындағы машиналық оқыту мен көпқабатты перцептрондарды модельдеу туралы еңбектері зерттеу жұмысының әдістемесін анықтауға мүмкіндік берді.

Зерттеу әдістері

Жалпы еліміздің алдыңғы қатарлы жоғары оқу орындарындағы «6В01511-Информатика» білім беру бағдарламалсының ақпараттық қауіпсіздік пәні бойынша силлабустарына қысқаша түрде талдау жүргізілді. Л.Н.Гумилев атындағы ЕҰУ, Яссауи атындағы ХТҚУ, Шәкәрім атындағы Семей МУ, А.Қуатбеков атындағы Халықтар достығы университтерінде «Ақпараттық қауіпсіздік негіздері» пәні 5 кредитті, ал М.Әуезов атындағы ОҚМУ, М.Өтемісов атындағы БҚМУ, Мырзахметов атындағы КМУ, Астана университеттерінде «Ақпараттық қауіпсіздік және ақпаратты қорғау» пәні 4 кредитті құрайды. Жалпы, пәннің мазмұны 5 кредитті қамтитын болса, онда 1 дәріс, 2 практикалық жұмыс және 2 сағат білім алушының өз бетінше жұмысын құрайды. Пәндердің білім мазмұны жалпылама мынадай тақырыптарды қамтитындығы анықталды: ақпараты қорғау мәселесінің өзектілігі мен негіздемесі, ақпаратты қорғау аймағындағы қауіпсіздік стандарттар мен бағдарламалар, ақпаратты қорғаудың концептуалды моделі, ақпараттық қауіпсіздікдің қауіп-қатер жүйесі, қаскүнем модель, заманауи қорғау технологиялары, вирусқа қарсы қорғау, заманауи қорғау технологиялары, желілік сүзгілеу, заманауи қорғау технологиялары, тунельдеу VPN арналарын қолдану, программалық интерактивтік орталар қызметтерін қолдану, ақпараттық қауіпсіздік мәдениетке қарасты тақырыптар. Демек, ақпараттық қауіпсіздікті жүзеге асыратын құралдар мен заманауи технологиялар толықтырылуы қажет.

Ақпараттық қауіпсіздік саласында машиналық оқыту алгоритмдерін қолдану Л.Н.Гумилев атындағы Еуразия ұлттық университетінің «6В01511-Информатика» білім беру бағдарламасының ақпараттық қауіпсіздікке байланысты арнайы курсының мазмұнын жетілдіру мақсатында қарастырылды. Оқыту әдісі ретінде топтық тәсіл қолданылды. Әрбір топқа жұмысты орындау үшін төмендегідей тізбекті алгоритм ұсынылды:

1) Google colab ортасында архивтелген файлдармен жұмыс жасау;
2) деректер базасында берілген деректердің өлшемін анықтау;
3) Tensorflow keras кітапханасын іске қосу;
4) деректерді оқыту;
5) нейронды желі арқылы кибершабуылдарды анықтау.

Деректерге шабуылдарды анықтау үшін көпқабатты персептрон MLP NN (Multi-Layer Perceptron Neural Network) архитектурасы қолданылды.

Көп қабатты перцептрон (MLP) – машиналық оқытуда қолданылатын қарапайым және кең таралған нейрондық желі архитектураларының бірі. Бұл өзара байланысқан нейрондардың бірнеше қабаттарынан, соның ішінде кіріс қабатынан, бір немесе бірнеше жасырын қабаттардан және шығыс қабатынан тұратын нейрондық желі. Көпқабатты персептрон кіріс және шығыс деректермен тікелей және кері таралу арқылы үйренеді. Оқытудың бұл түрі деректердің күрделі байланысттарын тіркеу және модельдеуге мүмкіндік береді. Көпқабатты перцептронның негізгі сипаттамаларын қарастырайық (Abd-elaziem, 2023: 37) [14]:

Кіріс деңгей: нейрондарды оқу процесі кіріс деңгейінен басталады.

Жасырын қабаттар: бұл қабаттардағы нейрондар кіріс деректерінде есептеулер жүргізеді. Әрбір нейронның шығысы оның кірістерінің өлшенген қосындысын қолдану, орын ауыстыруды қосу, содан кейін шыққан қосындыны белсендіру функциясы арқылы есептейді.

Шығыс қабат: классификация есептерінде бұл деңгейде softmax функциясын қолданылады.

Көпқабатты персептрондар толықтай өзара байланысқан болғандықтан, бір қабаттың әрбір түйіні келесі қабаттың түйінімен арнайы салмағымен байланысқан. Персептронда оқыту күтілетін нәтижемен салыстырғанда шығудағы қателер санына байланысты әрбір деректер фрагментін өңдегеннен кейін қосылыстардың салмағын өзгерту арқылы жүзеге асырылады. Бұл қатені кері тарату арқылы жүзеге асырылатын алгоритм бақыланатын оқытудың мысалы болып табылады.

Жоғарыдағы көп қабатты перцептрон диаграммасында біз төрт кіріс және жасырын

қабатта төрт түйін бар екенін көре аламыз. Шығу деңгейі төрт шығыс сигналын береді, яғни төрт шығыс түйіні бар. Кіріс деңгейіндегі түйіндер кірістерді қабылдайды және оларды әрі қарай өңдеу үшін жібереді, жоғарыдағы диаграммада кіріс деңгейіндегі түйіндер өз нәтижелерін үш түйіннің әрқайсысына жасырын деңгейде жібереді және сол сияқты жасырын деңгей ақпаратты өңдейді және оны шығыс деңгейіне жібереді.

Қабатты қабылдаудағы әрбір түйін сигма тәрізді белсендіру функциясын пайдаланады. Сигмойда белсендіру функциясы кіріс ретінде нақты мәндерді қабылдайды және оларды сигмойда формуласын пайдаланып 0-ден 1-ге дейінгі сандарға түрлендіреді (Grosse, 2024: 7) [15].

Көпқабатты персептрондардың жұмыс істеу негіздерін жүзеге асыру үшін Python ортасының TensorFlow кітапханасын пайдаланылатын боламыз.

Оқыту деректердің жиынтығы ретінде 694x201 деректер нүктесі бар элементтер қолданылды, ал тестілеу деректер жиынтығының өлшемі 15x201-ге тең.

Деректерді даярлау процесі аяқталған соң модель архитектурасын анықтаймыз. Біздің жағдайымызда көпқабатты персептрон архитектурасы қарастырылды. Бастапқы қажетті процестер жүзеге асырылған соң, мынадай келесі кезеңдерді қарастырамыз.

Модельді құрастыру: жоғалту функциясын, оңтайландырғышты және барлық тиісті көрсеткіштерді көрсету арқылы көпқабатты персептрон құрастырамыз.

Модельді оқыту: MLP дәуірлердің саны мен пакеттің өлшемін көрсете отырып, оқыту деректері бойынша үйретеміз.

Модельді бағалау: кез келген сәйкес көрсеткіштерді (мысалы, дәлдік, еске түсіру) есептеу арқылы сынақ деректері негізінде MLP өнімділігін бағалаймыз.

Нәтижелерді визуализациялау: оқу және валидация кезінде жоғалту және дәлдік графиктерін қолдана отырып, оқыту кезінде көпқабатты персептрон өнімділігін бейнелейміз.

Жіктеу мәселелерінде шығыс белгілері көбінесе категориялық болып табылады, яғни олар белгіленген кластар жиынтығына жатады. Жоғарыда айтылғандай, кодтау осы категориялық белгілерді 0s және 1s векторларына түрлендіру үшін қолданылады. Әрбір вектордың ұзындығы класстардың санымен бірдей және шынайы классқа сәйкес келетін индекстегі мән 1-ге, ал қалған барлық мәндер 0-ге тең болады. Модельдің шығыс деңгейі кластар бойынша ықтималдық үлестірімін берілетін болғандықтан, деректерді кластарға бөлу процесі маңызды болып табылады (Bento, 2021) [16]. Біздің жағдайымызда, Keras тегтерді бір реттік кодтауға түрлендіру үшін to_categorical деп аталатын қызметтік функцияны ұсынамыз:

```
from tensorflow import keras
model = keras.models.Sequential()
```

Нәтижесінде, 3 классқа(dense 1, dense2, dense 3) жіктеледі. Мұнда барлығы 26503 параметр болатын болса, оның 20503 параметрі оқыту үшін, ал қалғаны тестілеу үшін анықталды.

Кластарға жіктелген соң, жалпы қабаттары бар модельдерді анықтаймыз. Функционалды API (Application Programming Interface) күрделі модельдерден бірнеше кірісі немесе шығысы бар модельдерді немесе жалпы қабаттары бар модельдерді анықтауға мүмкіндік береді. Функционалды API пайдалану үшін алдымен кіріс қабатын анықтап, содан кейін кіріс қабатында оларды шақыратын қабаттар тізбегі жасалынады. Мұнда функционалды API көмегімен 200 және 150 бірліктен тұратын екі тығыз қабаты және softmax шығыс қабаты бар MLP құрылады.

Модельді Keras-қа құрастыру оңтайландырғышты, шығын функциясын және бағалау көрсеткішін көрсету арқылы модельді оқыту процесін орнатуды қамтамасыз етеміз.

Модельді оқыту барысында қолданылатын оңтайландырғыш, шығын функциясы мен бағалау көрсеткішіне қысқаша тоқталалсақ.

Шығын функциясы. Ол көп класты жіктеу тапсырмасы жағдайында кросс-энтропияның категориялық шығын функциясын қолданады. Бұл жоғалту функциясы болжанған ықтималдықтар мен шынайы класс белгілері арасындағы айырмашылықты өлшейді. Кросс-энтропияның категориялық жоғалуы көп класты жіктеу тапсырмалары үшін тиімді таңдау болып табылады, өйткені ол шығыс кластарының ықтималдық үлестірімін ескереді. Екілік жіктеу есебі үшін екілік кросс-энтропияның жоғалу функциясы, ал регрессия есебі үшін RMS (Retail Management System) жоғалту функциясы қолданылады (Rojas, 2022: 16) [17].

Көрсеткіштер (accuracy). Оқу және тестілеу кезінде модельдің өнімділігін бағалау үшін қолданылатын дәлдік көрсеткіші болып табы-

лады. Дәлдік үлгілердің жалпы санынан дұрыс жіктелген үлгілердің үлесін өлшейді. Бұл жіктеу тапсырмалары үшін кеңінен қолданылатын көрсеткіш, әсіресе кластар теңдестірілген кезде қолданылады. Бұл көрсеткіш машиналық оқытуды барлық алгоритмдерінде қолданылады (Brownlee, 2022) [18]. Орындалантын процесс барысында әрбір дерек бойынша 1-ші суретте көрсетілген код фрагментіне сәйкес 1000 іс-әрекет орындалды.

```
from keras import losses
model.compile(loss="categorical_crossentropy",
optimizer=keras.optimizers.Adam(learning_rate=0.00001, beta_1=0.9, beta_2=0.999, amsgrad=True),
metrics=["accuracy"])
hist = model.fit(Combined_training, target_total_train,epochs=1000, steps_per_epoch=2,validation_steps=2, validation_data = (Combined_testing,target_total_test))

Epoch 1/1000
2/2 [==============================] - 1s 221ms/step - loss: 69.3337 - accuracy: 0.0812 - val_loss: 93.9307 - val_accuracy: 0.3333
Epoch 2/1000
2/2 [==============================] - 0s 46ms/step - loss: 67.4461 - accuracy: 0.0821 - val_loss: 93.4087 - val_accuracy: 0.3333
Epoch 3/1000
2/2 [==============================] - 0s 53ms/step - loss: 65.5635 - accuracy: 0.0831 - val_loss: 92.8695 - val_accuracy: 0.3333
Epoch 4/1000
2/2 [==============================] - 0s 33ms/step - loss: 63.6911 - accuracy: 0.0845 - val_loss: 92.3114 - val_accuracy: 0.3333
```

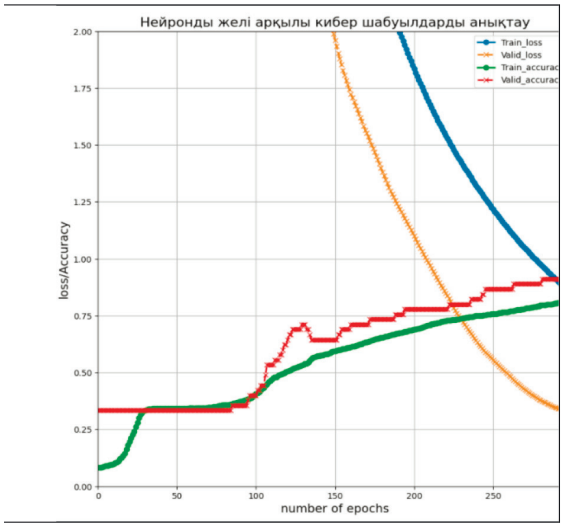
1-сурет – Модельді оқыту процесі

Мұндағы fit () функциясы берілген x_ train және y_train оқу деректері негізінде модельді оқыту үшін қолданылады. Batch_ size параметріне 2 мән беріледі, яғни оқыту деректері әрқайсысында 2 үлгіден тұратын пакеттерге бөлінеді. Fit () функциясы модельді 1000 ретінде берілген дәуірлердің берілген санына үйретеді. Модель салмақтары әр деректер пакетін өңдегеннен кейін жаңартылады және процесс көрсетілген «дәуір саны=1000» ішінде қайталанады. Құрылған модель негізінде нейронды желілердің көмегімен кибершабуылдарды анықтау үшін келесі код тізбегі қолданылады (2-сурет):

```
import pandas as pd
import matplotlib.pyplot as plt
plt.rcParams["figure.figsize"] = (10,10)
plt.plot(hist.history['loss'],label ="Train_loss",linestyle='solid', linewidth = 2,marker='o', markersize=6)
plt.plot(hist.history['val_loss'],label ="Valid_loss",linestyle='--', linewidth = 2,marker='x', markersize=6)
plt.plot(hist.history['accuracy'],label ="Train_accuracy",linestyle='solid', linewidth = 2,marker='o', markersize=6)
plt.plot(hist.history['val_accuracy'],label ="Valid_accuracy",linestyle='--', linewidth = 2,marker='x', markersize=6)
plt.gca().set_xlim(0, 300)
plt.gca().set_ylim(0, 2) # set the vertical range to [0-1]
plt.xlabel('number of epochs', fontsize=14)
plt.ylabel('loss/Accuracy', fontsize=14)
plt.title('Нейронды желі арқылы кибер шабуылдарды анықтау',fontsize=16)
plt.legend()
plt.grid(True)
```

2-сурет – Кибершабуылдарды анықтау кодының фрагменті

Нейронды желілердің көмегімен кибершабуылдарды анықтаудың нәтижесін график түрінде 3-ші суреттегідей ұсынамыз.



3-сурет – Кибершабуылдарды анықтаудың графиктік нәтижесі

Берілген функция оқу және валидация шығындарын, сондай-ақ оқу және валидация дәлдігін жоспарлау үшін ыңғайлы. Оның графикке арналған көрсеткіштер тізімі болып табылатын жалғыз міндетті аргументі бар. Мұндағы оқу және валидация шығындары бастапқыда төмендей бастағанын, ал көрсеткіш деңгейлерінің тұрақтылықты сақтайтындығын көре аламыз. Бұл модельдің оқу деректер жиынтығымен тиімді жұмыс істейтінін көрсетеді.

Әзірленген модельдің тиімділігін анықтау мақсатында SWOT талдау жүргізілді.

1-кесте – SWOT талдау нәтижесі

S Кибершабуылдарды анықтау моделі басқа да қауіп-қатерлерді анықтауға мүмкіндік береді; Кибершабуылдарды анықтау үшін модельді әзірлеудің алгоритмін білу.	W Модельге сәйкес мысал қарастыру; Модельді басқа да шабуылдарды анықтау үшін тестілеу.
O Әзірленген модельдің негізінде кибершабуылдарды анықтау; Модельді әзірлеу барысында қолданылған NLP әдісінен басқа, машиналық оқытудың басқа да алгоритмдерін қолдану.	T Басқа да типті кибершабуылдарды анықтау үшін модельдің тиімсіз болуы. Кибершабуылдарды анықтау барысында қателіктерге тап болу жағдайының анықталуы.

SWOT талдау жұмысы бойынша қорытынды жасайық. Модельдің күшті жақтары ретінде кибершабуылдарды анықтау моделі басқа да қауіп-қатерлерді анықтауға мүмкіндік беруі мен кибершабуылдарды анықтау үшін модельді әзірлеудің алгоритмін білуді жатқызамыз. Демек, әзірленген модельге негізделе білім алушылар басқа да кибершабуылдарды анықтаудың моделін құруға, шабуылдарды анықтау мүмкіндік алады. Әлсіз жақтары ретінде модельге сәйкес нақты шабуылдарды анықтайтын мысалдарды қарастырмау жатады. Яғни, егер де мысал қарастыру барысында қандай да бір қателік анықталса, онда модельдің жарамсыздығы анықталады. Сондай ақ, модельдің мүмкіндіктері ретінде әзірленген модельдің негізінде кибершабуылдарды анықтау мен модельді әзірлеу барысында қолданылған NLP әдісінен басқа, машиналық оқытудың басқа да алгоритмдерін қолдануды жатқызуға болады, яғни бұл модельде қарастырылған алгоритм білім алушыға Python ортасында қандай да бір процесті анықтау(болжау) моделдерін құру түсінігін қалыптастырады. Ал, модельдің қауіп-қатерлері ретінде басқа да типті кибер-

шабуылдарды анықтау үшін модельдің тиімсіз болуы мен кибершабуылдарды анықтау барысында қателіктерге тап болу жағдайының анықталуын жатқызамыз, яғни қандай да бір қателіктер пайда болатын болса, онда модель тиімсіз болып табылады. Әзірленген модельдің әлсіз жақтары мен қауіп-қатерлеріне қарамастан оның күшті жақтары мен мүмкіндіктерін талдай келе, ол білім алушыларға кибершабуылдарды анықтау үшін модель әзірлеу түсініктерін қалыптастыруға, ақпараттық қауіпсіздік саласы бойынша білімдерін жетілдіруге мүмкіндік береді деп тұжырымдаймыз.

Ақпараттық қауіпсіздік бойынша арнайы пән курсының мазмұнын жетілдіру мақсатында машиналық оқыту алгоритмдері көмегімен мынадай типтес практикалық сағаттар енгізілетін болады: спамды анықтау, қауіптерді ерте кезеңде анықтау, желінің осалдылықтарын анықтау, ақпараттық технологиялардың жұмыс жүктемелері мен шығындарын азайту, нейронды желі көмегімен кибершабуылды анықтау, Wireshark көмегімен желіні бақылау, Nmap (ақпарат жинау), анонимді FTP сканерін пайдалану, жойылған файлдарды анықтау, Zip құпия сөзін бұзушы, Brute Force FTP, порт сканері. Аталған практикалық жұмыстарды жүзеге асыру нәтижесі ақпараттық қауіпсіздік саласы бойынша білім алушыларға мынадай дағдыларды қалыптастыруға мүмкіндік береді:

1) нақты уақыт режимінде желілік қатерлерді қателіксіз алдын-ала анықтай алу мүмкіндігі;

2) машиналық оқыту көмегімен ақпараттық қауіпсіздік мәселелерін шешуде басқа пән (салалармен) интеграциялану мүмкіндігі, яғни Matlab, Python сияқты орталармен жұмыс істеу мүмкіндігі;

3) ақпараттық қауіпсіздік мәселелерінің нақты қалай жұмыс істейдігін түсіну;

4) үлкен көлемді деректерді жылдам жалпылай алу мүмкіндігі; аналитиктерге қандай да бір болжам жасау барысында ең үлкен қиындық туғызатын проблемалардың бірі – барлау жұмыстарын жылдамдату, ал, машиналық оқыту тарихи және динамикалық ақпараттың үлкен көлемін тез талдай алады; командаларға нақты уақыт режимінде әр түрлі көздерден деректерді өңдеуге мүмкіндік береді;

5) қолмен орындалатын қайталанатын тапсырмаларды аутоматтандыра алуы; белгілі бір тапсырмаларға машиналық оқытуды қолдану қауіпсіздік топтарын күнделікті, қайталанатын тапсырмалардан арылтуға көмектеседі; кіріс ескертулеріне жауап беру әрекеттерін масштабтауға және уақыт пен ресурстарды күрделі стратегиялық жобаларға бағыттауға мүмкіндік береді;

6) машиналық оқытудың нақты уақыт режимінде аналитикалық ақпаратты өзекті деректермен толықтыра алуы – қауіп-қатерлерді іздеуге және қауіпсіздік операцияларына қатысатын аналитиктерге өз ұйымының маңызды осалдықтарын жою үшін ресурстарға тиімді басымдық беруге мүмкіндік береді.

Нәтижелер және талқылау

Ақпараттық қауіпсіздік саласында машиналық оқыту алгоримдерін қолдану тиімділігін анықтау мақсатында Л.Н. Гумилев атындағы Еуразия ұлттық университетінің «6В01511-Информатика» білім беру бағдарламасының білім алушыларына экспериментке дейін және эксперименттен кейін сауалнамалық жұмыстар жүргізілді. Сауалнамалық жұмыстардың негізгі мазмұны ақпараттық қауіпсіздік саласындағы машиналық оқыту алгоритмдерінің маңыздылығы, тиімділігі сияқты сұрақтарды қамтиды. Эксперимент өткенге дейінгі және өткеннен кейінгі сауалнама нәтижесін қарастырайық (2-кесте). 2-ші кестеден көріп отырғанымыздай, пәннің мазмұнына экспериментке дейін 11% білім алушы қанағаттанса, эксперименттен кейін 66% білім алушы қанағаттанушылық танытқан. Бұл дегеніміз, арнайы пән курсының мазмұнын жетілдіру сәтті жүзеге асырылды деген тұжырымды береді. Сәйкесінше, пәннің заманауи проблемаларды қарастыру деңгейі мен пәндік интеграциялану деңгейі де 10%-ға жоғарылаған. Ал, сабақ барысында қолданылатын оқытудың әдіс-тәсілдерін, формаларын қолдану деңгейі шамамен өзгеріссіз қалған. Арнайы пән курсының мазмұнын жетілдіру нәтижесінде білім алушылардың практикалық дағдыларды қалыптастыру деңгейінің 55%-ға жоғарылағанын байқаймыз.

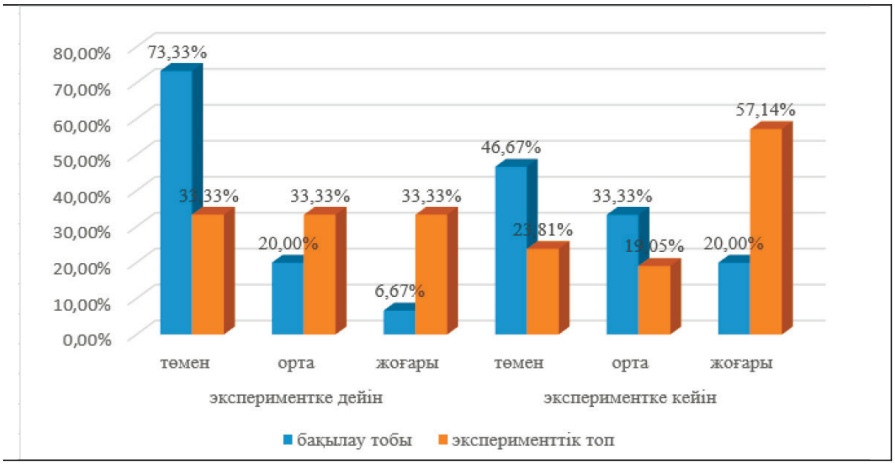
2-кесте – Сауалнама нәтижесі

№	Бағалау критерийлері	Экспериментке дейін					Эксперименттен кейін				
		Бағалау, балл (пайызбен)					Бағалау, балл (пайызбен)				
		1	2	3	4	5	1	2	3	4	5
1	Пәннің мазмұнына қанағаттану деңгейі	0	6	32	51	11	0	0	21	13	66
2	Заманауи проблемаларды қарастыру деңгейі	0	8	50	30	12	0	5	25	35	35
3	Пәндік интеграция деңгейі	5	10	25	25	25	0	5	20	40	35
4	Аппараттық қамтамасыздандыруды қолдану деңгейі	32	38	20	10	0	10	15	15	30	30
5	Программалық қамтамасыздандыруды қолдану деңгейі	0	0	0	45	55	0	0	0	35	65
6	Заманауи педагогикалық әдіс-тәсілдерді қолдану деңгейі	0	0	0	48	52	0	0	0	45	55
7	Практикалық дағдыларды қалыптастыру деңгейі	0	0	15	25	60	0	0	10	15	75

Демек, зерттеу жұмысы барысында ақпараттық-коммуникациялық технологияларды заман ағымына сай дамуына байланысты ақпараттық қауіпсіздік саласы бойынша оқу мазмұнының жетілдірілуі оң әсерін берді деп нақты айта аламыз. Топтық жұмыс барысында бақылау(ақпараттық қауіпсіздік пәнінің мазмұны жетілдірілмеген) және эксперименттік топтар(ақпараттық қауіпсіздік пәнінің мазмұны жетілдірілген) тағайындалды (4- сурет).

Нөлдік: егер ақпараттық қауіпсіздік бойынша пәннің мазмұны жетілдіріліп, ЖОО-ның оқу процесінде іске асырылса, онда жоғары оқу орындарының білім алушыларында ақпараттық қауіпсіздік саласы бойынша білім сапасының артуына әсері болмайды;

Альтернативті: егер ақпараттық қауіпсіздік бойынша пәннің мазмұны жетілдіріліп, ЖОО-ның оқу процесінде іске асырылса, онда жоғары оқу орындарының білім алушыларында ақпараттық қауіпсіздік саласы бойынша білім сапасы артады.



4-сурет – Эксперименттік жұмыстардың графиктік нәтижесі

1) минималды және максималды кибершабуылдары бар жабық цикл деректері жинақталды;

2) нейронды желі моделінің архитектурасы анықталды;

3) деректер кластарға жіктелді;

4) жіктелген деректердің негізінде модель оқытылды;

5) нейронды желі негізінде кибершабуылдар анықталды.

Қорытынды

Әзірленген модельдің тиімділігін анықтау мақсатында SWOT-талдау жұмыстары анықталды. Нәтижесінде, кибершабуылдарды анықтау моделі білім алушыларға кибершабуылдарды анықтау моделін әзірлеу түсініктерін қалыптастыруға, ақпараттық қауіпсіздік саласы бойынша білімдерін жетілдіруге мүмкіндік береді деп тұжырымдалады. Сонымен қатар, әзірленген машиналық оқытуда нейронды желі моделін әртүрлі салада, кез-келген процесті анықтау үшін қолдануға болады. Бұл процес «6В01511-Информатика» білім беру бағдарламасының ақпараттық қауіпсіздікке байланысты арнайы курсының мазмұнын жетілдіру мақсатында жүзеге асырылды. Сауалнама қорытындылары бойынша осындай типті зерттеу жұмыстарын арнайы курсқа енгізу нәтижесі оң әсерін беретіндігін анықтайды. Сондай-ақ, бақылау(ақпараттық қауіпсіздік пәнінің мазмұны жетілдірілмеген) және эксперименттік топтар (ақпараттық қауіпсіздік пәнінің мазмұны жетілдірілген) негізінде жүргізілген эксперименттік жұмыстардың нәтижесі бойынша ақпараттық қауіпсіздік пәнінің мазмұнын жетілдіру арқылы білім алушылардың ақпараттық қауіпсіздік саласы бойынша білім сапасы арттыра аламыз.

Әдебиеттер

1. Dasgupta D., Akhtar Z., Sen S. Machine learning in cybersecurity: a comprehensive survey //The Journal of Defense Modeling and Simulation. – 2022. – Т. 19. – №. 1. – С. 57-106

2. Apruzzese G. et al. The role of machine learning in cybersecurity //Digital Threats: Research and Practice. – 2023. – Т. 4. – №. 1. – С. 1-38.

3. Momcheva G., Sabra A., Rmeiti N. Machine learning in Cybersecurity. – 2022.

4. Manjramkar M. A., Jondhale K. C. Cyber Security Using Machine Learning Techniques //International Conference on Applications of Machine Intelligence and Data Analytics (ICAMIDA 2022). – Atlantis Press, 2023. – С. 680-701.

5. Kantamsetti P. Machine Learning applications in the field of cyber security //Machine Learning. – 2021. – Т. 8. – №. 8.

6. Bharadiya J. Machine Learning in Cybersecurity: Techniques and Challenges //European Journal of Technology. – 2023. – Т. 7. – №. 2. – С. 1-14.

7. Suresh P. et al. Contemporary survey on effectiveness of machine and deep learning techniques for cyber security //Machine Learning for Biometrics. – Academic Press, 2022. – С. 177-200.

8. Shaukat K. et al. A survey on machine learning techniques for cyber security in the last decade //IEEE access. – 2020. – Т. 8. – С. 222310-222354.

9. Ahsan M. et al. Cybersecurity threats and their mitigation approaches using Machine Learning—A Review //Journal of Cybersecurity and Privacy. – 2022. – Т. 2. – №. 3. – С. 527-555.

10. Popescu M. C. et al. Multilayer perceptron and neural networks //WSEAS Transactions on Circuits and Systems. – 2009. – Т. 8. – №. 7. – С. 579-588.

11. Toha S. F., Tokhi M. O. MLP and Elman recurrent neural network modelling for the TRMS //2008 7th IEEE international conference on cybernetic intelligent systems. – IEEE, 2008. – С. 1-6.

12. Carlsson L. E. O. Using Multilayer Perceptrons asmeans to predict the end-pointtemperature in an Electric ArcFurnace. – 2015.

13. Abu-Doush I. et al. Enhancing multilayer perceptron neural network using archive-based harris hawks optimizer to predict gold prices //Journal of King Saud University-Computer and Information Sciences. – 2023. – Т. 35. – №. 5. – С. 101557.

14. Abd-elaziem A. H., Soliman T. H. M. A Multi-Layer Perceptron (MLP) Neural Networks for Stellar Classification: A Review of Methods and Results‖ //International Journal of Advances in Applied Computational Intelligence. – Т. 3. – №. 10.54216.

15. Grosse R. Lecture 5: Multilayer Perceptrons //inf. téc. – 2019.

16. Bento C. Multilayer perceptron explained with a real-life example and python code: Sentiment analysis //Towards Data Science. – 2021.

17. Rojas M. G., Olivera A. C., Vidal P. J. Optimising Multilayer Perceptron weights and biases through a Cellular Genetic Algorithm for medical data classification //Array. – 2022. – Т. 14. – С. 100173.

18. Brownlee J. Crash Course on Multi-Layer Perceptron Neural Networks. 2022.

References

Abd-elaziem, A. H., & Soliman, T. H. A Multi-Layer Perceptron (MLP) Neural Networks for Stellar Classification: A Review of Methods and Results‖. International Journal of Advances in Applied Computational Intelligence, 3(10.54216).

Abu-Doush, I., Ahmed, B., Awadallah, M. A., Al-Betar, M. A., & Rababaah, A. R. (2023). Enhancing multilayer perceptron neural network using archive-based harris hawks optimizer to predict gold prices. Journal of King Saud University-Computer and Information Sciences, 35(5), 101557.

Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity threats and their mitigation approaches using Machine Learning—A Review. Journal of Cybersecurity and Privacy, 2(3), 527-555.

Apruzzese, G., Laskov, P., Montes de Oca, E., Mallouli, W., Brdalo Rapa, L., Grammatopoulos, A. V., & Di Franco, F. (2023). The role of machine learning in cybersecurity. Digital Threats: Research and Practice, 4(1), 1-38.

Bento C. (2021, September 21). Multilayer perceptron explained with a real-life example and python code: Sentiment analysis. Towards Data Science. https://towardsdatascience.com/multilayer-perceptron-explained-with-a-real-life-example-and-python-code-sentiment-analysis-cb408ee93141

Bharadiya, J. (2023). Machine learning in cybersecurity: Techniques and challenges. European Journal of Technology, 7(2), 1-14.

Brownlee, J. Crash Course on Multi-Layer Perceptron Neural Networks. 2022.

Carlsson, L. E. O. (2015). Using Multilayer Perceptrons asmeans to predict the end-pointtemperature in an Electric ArcFurnace.

Dasgupta, D., Akhtar, Z., & Sen, S. (2022). Machine learning in cybersecurity: a comprehensive survey. The Journal of Defense Modeling and Simulation, 19(1), 57-106.

Grosse, R. (2019). Lecture 5: Multilayer Perceptrons. inf. tec.

Kantamsetti, P. (2021). Machine Learning Applications in the Field of Cyber Security. International Journal of Innovations in Engineering Research and Technology, 8(08), 103-110.

Manjramkar, M. A., & Jondhale, K. C. (2023, May). Cyber Security Using Machine Learning Techniques. In International Conference on Applications of Machine Intelligence and Data Analytics (ICAMIDA 2022) (pp. 680-701). Atlantis Press.

Momcheva, G., Sabra, A., & Rmeiti, N. (2022). Machine Learning in cybersecurity.

Popescu, M. C., Balas, V. E., Perescu-Popescu, L., & Mastorakis, N. (2009). Multilayer perceptron and neural networks. WSEAS Transactions on Circuits and Systems, 8(7), 579-588.

Rojas, M. G., Olivera, A. C., & Vidal, P. J. (2022). Optimising Multilayer Perceptron weights and biases through a Cellular Genetic Algorithm for medical data classification. Array, 14, 100173.

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020). A survey on machine learning techniques for cyber security in the last decade. IEEE access, 8, 222310-222354.

Suresh, P., Logeswaran, K., Keerthika, P., Devi, R. M., Sentamilselvan, K., Kamalam, G. K., & Muthukrishnan, H. (2022). Contemporary survey on effectiveness of machine and deep learning techniques for cyber security. In Machine Learning for Biometrics (pp. 177-200). Academic Press.

Toha, S. F., & Tokhi, M. O. (2008, September). MLP and Elman recurrent neural network modelling for the TRMS. In 2008 7th IEEE international conference on cybernetic intelligent systems (pp. 1-6). IEEE.

Авторлар туралы мәлімет:

Серік Меруерт(корреспонденттік автор)- педагогика ғылымдарының докторы, Л.Н.Гумилев атындағы Еуразия Ұлттық университеті Информатика кафдерасының профессоры (Астана қ., Қазақстан, эл. пошта: serik_meruerts@mail.ru);

Тлеумагамбетова Данара Шайкуалиевна- техника ғылымдарының магистрі, Л.Н.Гумилев атындағы ЕҰУ «8D01511-Информатика» білім беру бағдарламасының 2 курс докторанты(Астана қ. Қазақстан, эл. пошта: danara1310@gmail.com);

Құрымбаев Саят Гайниевич- педагогика ғылымдарының кандидаты, Академик Е.А.Букетов атындағы Қарағанды университеті Транспорт және логистикалық жүйелер кафедрасының доценті (Қарағанды қ., Қазақстан, эл.пошта: sakura3874@mail.ru).

Самашова Гульфарида Ергалиевна- педагогика ғылымдарының кандидаты, А. Сағынов атындағы Қарағанды техникалық университеті, Ақпараттық технологиялар факультетінің деканы, Кәсіби білім беру және педагогика кафедрасының доценті(Қарағанды қ. , Қазақстан, эл.пошта: gsamash74@mail.ru)

Сведения об авторах:

Серик Меруерт (корреспондентный автор) – доктор педагогических наук, професссор кафедры Информатика Евразийского Национального университета им. Л.Н.Гумилева (г. Астана Казахстан, эл.почта: serik_meruerts@mail.ru);

Тлеумагамбетова Данара Шайкуалиевна – магистр технических наук наук, докторант 2 курса образовательной программы «8D01511-Информатика» Евразийского Национального университета (г. Астана Казахстан, эл.почта: danara1310@gmail.com);

Курымбаев Саят Гайниевич- кандидат педагогических наук, доцент кафедры Транспорта и логистических систем Карагандинского университета им. Академика Е.А. Букетова (г. Караганда Казахстан, эл.почта: sakura3874@mail.ru);

Самашова Гульфарида Ергалиевна- кандидат педагогических наук, декан факультета Информационной технологии, доцент кафедры Профессионального образования и педагогики Карагандинского технического университета им. А. Сагынова (г. Караганды, Казахстан, эл.почта: gsamash74@mail.ru).

Information about authors:

Serik Meruyert (corresponding author) – Doctor of Pedagogical Sciences, Professor of the Department of Computer Science of L.N. Gumilyov Eurasian National University (Astana, Kazakhstan, e-mail: serik_meruerts@mail.ru);

Tleumagambetova Danara- Master of Technical Sciences, Doctoral student of educational program «8D01511 – Computer science» of L.N. Gumilyov Eurasian National University(Astana, Kazakhstan, e-mail: danara1310@gmail.com);

Kurymbayev Sayat- Candidate of Pedagogical Sciences, Associate Professor of the Department of Transport and Logistics Systems of Karaganda Buketov University (Karaganda, Kazakhstan, e-mail: sakura3874@mail.ru);

Samashova Gulfarida- Candidate of Pedagogical Sciences, Dean of the Faculty of Information Technology, Associate Professor of the Department of Vocational Education and Pedagogy of the A. Sagynov Karaganda Technical University (Karaganda, Kazakhstan, e-mail: gsamash74@mail.ru).

Келіп түсті 23.01.2024
Қабылданды 01.03.2024