ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE

№1
2026

ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

CENTRAL ASIAN ACADEMIC
RESEARCH CENTER

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE

1 (357)

JANUARY – MARCH 2026

PUBLISHED SINCE JANUARY 1963
PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

Academic Scientific Journal of Computer Science
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Owner: «Central Asian Academic Research Center» LLP (Almaty).
Certificate **№ KZ77VPY00121154** on the re-registration of the periodical printed and online publication of the information agency, issued on **05.06.2025** by the Republican State Institution «Information Committee» of the Ministry of Culture and Information of the Republic of Kazakhstan
Subject area*: information and communication technologies.*
Currently: *included in the list of journals recommended by the CCSES MSHE RK in the direction of «Information and communication technologies».*
Periodicity: *4 times a year.*
http://www.physico-mathematical.kz/index.php/en/

Academic Scientific Journal of Computer Science
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Меншіктеуші: «Орталық Азия академиялық ғылыми орталығы» ЖШС (Алматы).
Ақпарат агенттігінің мерзімді баспасөз басылымын, ақпарат агенттігін және желілік басылымды қайта есепке қою туралы ҚР Мәдениет және Ақпарат министрлігі «Ақпарат комитеті» Республикалық мемлекеттік мекемесі **05.06.2025** ж. берген **№ KZ77VPY00121154** Куәлік.
Тақырыптық бағыты: *ақпараттық-коммуникациялық технологиялар*
Қазіргі уақытта: *«ақпараттық-коммуникациялық технологиялар» бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*
Мерзімділігі: *жылына 4 рет.*
http://www.physico-mathematical.kz/index.php/en/

Academic Scientific Journal of Computer Science
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Собственник: *ТОО «Центрально-азиатский академический научный центр» (г. Алматы).*
Свидетельство о постановке на переучет периодического печатного издания, информационного агентства и сетевого издания **№ KZ77VPY00121154.** Дата выдачи **05.06.2025**
Тематическая направленность: *информационно-коммуникационные технологии.*
В настоящее время: *вошел в список журналов, рекомендованных КОКСНВО МНВО РК по направлению «информационно-коммуникационные технологии».*
Периодичность: *4 раза в год.*
http://www.physico-mathematical.kz/index.php/en/

CONTENTS

COMPUTER SCIENCE

Akhmetova S.T., Yunussova A.A., Alisheva S.S., Olzhataeva B.T., Mussirepova E.B.
Social network data mining for automated offensive language detection.....13

Amanov A.N., Kazbekova G.N., Zhunissov N.M., Abibullayeva A.A., Aben A.B.
Artificial intelligence-based intrusion detection for DDOS attacks in Software Defined Networking.....30

Amanzholova S.T., Ussatova O.A., Mutanov G.M., Mukhanov S.B., Aitmukash D.
Backend architecture of a hybrid blockchain-based academic credential verification system.....52

Amirkhanova G.A., Nurgazy T.N., Amirkhanov B.S., Tokhtassyn M.M., Nurgazy N.N.
Developing a predictive digital twin for a food product based on Edge ML and IoT sensors.....73

Bekarystankyzy A., Ussen D., Kassenkhan A., Chinibayev Y.
Cold-start in educational recommender systems: classical and LLM-Era strategies.....91

Bimoldina Zh., Mussiraliyeva Sh., Bagitova K., Tereikovska L.
Detection of cyber-propaganda content using machine learning and semantic models....106

Chezhimbayeva K.S.
Forecasting key 5G network KPIs using MLP and LSTM neural network models.....129

Dauitbayeva A.O., Konyrbaev N.B., Abildayeva Zh.T., Yessirkepova A.U., Karim N.A.
Development of an application to optimize the process of employment of graduates.....148

Dzhsupbekova G., Othman M., Ordabayeva G.
Comparative analysis of artificial intelligence algorithms to detect network attacks.....167

Issakhov A., Orazmoldayev N., Zharkynbek Y., Abylkassymova A.
Numerical modeling of the spread of viral infection by airborne droplets in confined spaces.....182

Kantureeva M., Omarova G.S., Duisen Z.D., Shekerbek A.A., Tulebayev Y.B.
Application of machine learning methods in forecasting and optimizing the processes of evacuation of people in high-rise buildings.....202

Khusain B., Telmanov M., Khusain A.B., Brodskiy A.R., Sass A.S.
Digital twin of an integrated emission purification and decarbonization system for thermal units.....218

Kulakayeva A., Ashurov A., Zhumazhanov B., Daineko Ye., Zylgara A.
Algorithm for determining the initial orbital parameters of KazeEOSat-1 for deorbiting.....236

Mimenbayeva A.B., Turebayeva R.D., Ospanova T.T., Aruova A.B., Naizagarayeva A.A.
Development and comparative analysis of machine learning models for urban traffic prediction.....253

Naumenko V.V., Mukanova Zh.A., Kiseleva O.V., Maintser D.A., Nerezov A.K.
The use of real-time polling to improve student academic performance.....271

Nazyrova A.E., Kaderkeyeva Z.K., Bekmanova G.T., Milosz M., Lamasheva Zh.
Transformation of education through digital technologies: advancing student academic performance across learning stages.....287

Oralbekova D., Mamyrbayev O., Akhmediyarova A., Kassymova D., Alibiyeva Z.
Development of a multi-level model for text summarization based on pretrained models.....316

Orazbayev B.B., Zhumadillayeva A.K., Kurbangalieva N.B., Yessirkessinov R.Zh., Orazbayeva K.N.
Synthesis of linguistic models for assessing sulfur quality and fuzzy modeling of the sulfur production process.....337

Sarsenbayeva A.K., Rakhimova D.R., Shormakova A.N., Mansurova M.E., Adali E.
Application of semantic methods in the field of legislation: an intellectual system for analysis of agglutinative texts.....354

Serek A., Shoiynbek A., Sharipov K., Kuanyshbay D., Mukhametzhanov A.
Analysis and classification of telephone fraud based on lexical features of speech transcriptions.....373

Shynzhigit B.B., Balabekova M.O., Amangeldy T.T.
Analysis and forecasting of brick product sales using machine learning models.....393

Tokhayeva A.O., Alzhanov A.K., Nezih Önal, Ziyatbekova G.Z., Begalieva K.B.
Formation of students virtualization competencies in higher education based on Proxmox VE.....412

Tukenova L.M., Auyelbekov O.A., Sapakova S.Z., Sametova A.A., Bostanov E.L.
Modelling and optimisation of hybrid power plant operating modes for unmanned aerial vehicles.....430

Yerimbetova A., Berzhanova U., Daiyrbayeva E., Sakenov B., Sambetbayeva M.
Sign language recognition using temporal convolutional network and MediaPipe.....443

Zhukabayeva T.K., Benkhelifa E., Mardenov Y.M., Baumuratova D., Karabayev N.
Decision support for responding to attacks in cyber-physical industrial internet-of-things systems.....461

МАЗМҰНЫ

ИНФОРМАТИКА

Ахметова С.Т., Юнусова А.А., Алишева С.С., Олжатаева Б.Т., Мүсірепова Э.Б.
Әлеуметтік желідегі бейәдеп пікірлерді автоматты анықтауда деректерді интеллектуалды талдау.....13

Аманов А.Н., Казбекова Г.Н., Жунисов Н.М., Абибуллаева А.А., Абен А.Б.
Бағдарламалық жасақтамамен анықталған желідегі DDOS шабуылдары үшін жасанды интеллектке негізделген шабуылдарды анықтау.....30

Аманжолова С.Т., Усатова О.А., Мутанов Г.М., Муханов С.Б., Айтмукаш Д.
Гибридтік блокчейнге негізделген академиялық сенімдік деректерді тексеру жүйесінің бекендік архитектурасы.....52

Амирханова Г.А., Нұрғазы Т.Н., Амирханов Б.С., Нұрғазы Н. Н.
EDGE ML және IOT сенсорлары негізінде азық-түлік өнімінің предиктивті цифрлық егізін әзірлеу.....73

Бекарыстанқызы А., Үсен Д., Қасенхан А., Чинибаев Е.
Білім беру саласындағы ұсынымдық жүйелеріндегі «Cold-start» мәселесі: классикалық әдістер және LLM дәуірінің стратегиялары.....91

Бимолдина Ж.А., Мусиралиева Ш.Ж., Багитова К.Б., Терейковская Л.З
Кибернасихаттық контентті анықтау үшін машиналық оқыту және семантикалық модельдер қолдану.....106

Чежимбаева К.С.
MLP және LSTM нейрондық желі модельдерін қолдана отырып, 5G желісінің негізгі KPI-лерін болжау.....129

Дәуітбаева А.О., Қоңырбаев Н.Б., Әбілдаева Ж.Т., Есіркепова А.У., Кәрім Н.Ә.
Бітіруші түлектердің жұмысқа орналастыру процесін оңтайландыру үшін қосымша әзірлеу.....148

Джусупбекова Г., Othman M., Ордабаева Г.
Жасанды интеллект алгоритмдерін желілік шабуылдарды анықтау үшін салыстырмалы талдау.....167

Исахов А.А., Оразмолдаев Н., Жаркынбек Е., Абылкасымова А.
Ауа тамшылары арқылы вирустық инфекцияның шектеулі кеңістікте таралуын сандық модельдеу.....182

Кантуреева М.А., Омарова Г.С., Дүйсен Ж.Д., Шекербек А.Ә., Тулебаев Е.Б.
Биік ғимараттардағы адамдарды эвакуациялау процестерін болжау және оңтайландыруда машиналық оқыту әдістерін қолдану.....202

Хусаин Б., Тельманов М.М., Хусаин А.Б., Бродский А.Р., Сасс А.С.
Жылу қондырғыларының шығарындыларын кешенді тазалау және
декарбонизациялау жүйесінің цифрлық егізі.....218

Кулакаева А.Е., Ашуров А.Е., Жумажанов Б.Р., Дайнеко Е.А., Зылғара А.Е.
KAZEOSAT-1 ғарыш аппаратының деорбитациясын жүзеге асыру үшін
бастапқы орбиталық параметрлерін анықтау алгоритмі.....236

Мименбаева А.Б., Туребаева А.Д., Оспанова Т.Т., Аруова А.Б.,
Найзағараева А.А.
Қалалық көлік ағынын болжауға арналған машиналық оқыту модельдерін
әзірлеу және салыстырмалы талдау.....253

Науменко В.В., Муканова Ж.А., Киселева О.В., Майнцер Д.А., Нерезов А.К.
Білім алушылардың үлгерімін арттыру үшін real-time
сауалнамаларын қолдану.....271

Назырова А.Е., Кадеркеева З.К., Бекманова Г.Т., Милош М., Ламашева Ж.Б.
Цифрлық білім және студенттердің академиялық жетістіктері:
деңгейлер бойынша білім беруді дамыту.....287

Оралбекова Д., Мамырбаев О., Ахмедиярова А., Қасымова Д.З, Алибиева Ж.,
Алдын ала оқытылған модельдер негізінде мәтінді резюмелеуге
арналған көпдеңгейлі модельді әзірлеу.....316

Оразбаев Б.Б., Жумадиллаева А.К., Курбангалиева Н.Б., Оразбаева К.Н.
Күкірт сапасын бағалаудың лингвистикалық модельдерін синтездеу
және күкіртті өндіру процесін бұлыңғыр модельдеу.....337

Сарсенбаева А.К., Рахимова Д.Р., Шормакова А.Н., Мансурова М.Е., Адали Э.
Семантикалық әдістерді заңнама саласында қолдану: агглютинативті
мәтіндерді талдауға арналған интеллектуалды жүйе.....354

Серек А., Шойынбек А., Шарипов К., Қуанышбай Д., Мухаметжанов А.
Сөйлеу транскрипцияларының лексикалық белгілеріне негізделген телефон
алаяқтықтарын талдау және жіктеу.....373

Шынжігіт Б.Б., Балабекова М.О., Амангелді Т.Т.
Кірпіш өнімдерін сату көлемдерін машиналық оқытуда талдау
және болжамдау.....393

Тохаева А.О., Альжанов А.К., Nezih Ö., Зиятбекова Г.З., Бегалиева К.Б.
PROXMOX VE негізінде жоғары оқу орындарында білім алушыларды
виртуалдандыру құзыреттерін қалыптастыру.....412

Төкенова Л.М., Әуелбеков О.А., Сапақова С., Саметова А.А., Бостанов Е.Л.
Пилотсыз ұшу аппараттарына арналған гибридті электр станцияларының жұмыс режимдерін модельдеу және оңтайландыру.....430

Еримбетова А.С., Бержанова У.Г., Дайырбаева Э.Н., Сәкенов Б.Е., Самбетбаева М.А.
Уақытша конволюциялық желі мен mediaріре көмегімен ым тілін тану.....443

Жукабаева Т.К., Бенхелифа Э., Марденов Е.М., Баумуратова Д., Карабаев Н.
Киберфизикалық өнеркәсіптік интернет заттары жүйелеріндегі шабуылдарға әрекет ету кезінде шешім қабылдауды қолдау.....461

СОДЕРЖАНИЕ

ИНФОРМАТИКА

Ахметова С.Т., Юнусова А.А., Алишева С.С., Олжатаева Б.Т., Мүсірепова Э.Б.
Интеллектуальный анализ данных для автоматического выявления языка ненависти в социальных сетях.....13

Аманов А.Н., Казбекова Г.Н., Жунисов Н.М., Абибуллаева А.А., Абен А.Б.
Обнаружение вторжений на основе искусственного интеллекта для DDoS-атак в программно-определяемых сетях.....30

Аманжолова С.Т., Усатова О.А., Мутанов Г.М., Муханов С.Б., Айтмукаш Д.
Бэкенд-архитектура гибридной системы проверки академических достижений на основе блокчейна.....52

Амирханова Г.А., Нургазы Т.Н., Амирханов Б.С., Нургазы Н.Н.
Разработка предиктивного цифрового двойника пищевого продукта на основе Edge ML и IoT-сенсоров.....73

Бекарыстанқызы А., Үсен Д., Қасенхан А., Чинибаев Е.
Холодный старт в системах рекомендаций в области образования: классические подходы и стратегии эпохи LLM.....91

Бимолдина Ж.А., Мусиралиева Ш.Ж., Багитова К.Б., Терейковская Л.
Использование машинного обучения и семантических моделей для обнаружения киберпропагандистского контента.....106

Чежимбаева К.С.
Прогнозирование ключевых KPI сетей 5G на основе нейросетевых моделей MLP и LSTM.....129

Даутбаева А.О., Конырбаев Н.Б., Абильдаева Ж.Т., Есиркепова А.У., Карим Н.А.
Разработка приложения для оптимизации процесса трудоустройства выпускников.....148

Джусупбекова Г., Othman M., Ордабаева Г.
Сравнительный анализ алгоритмов искусственного интеллекта для обнаружения сетевых атак.....167

Исахов А.А., Оразмолдаев Н., Жаркынбек Е., Абылкасымова А.
Численное моделирование распространения вирусной инфекции воздушно-капельным путём в замкнутых помещениях.....182

Кантуреева М.А., Омарова Г.С., Дүйсен Ж.Д., Шекербек А.Ә., Тулебаев Е.Б.
Использование методов машинного обучения для прогнозирования
и оптимизации процессов эвакуации людей в высотных зданиях.....202

Хусаин Б., Тельманов М.М., Хусаин А.Б., Бродский А.Р., Сасс А.С.
Цифровой двойник комплексной системы очистки и декарбонизации
выбросов тепловых установок.....218

Кулакаева А.Е., Ашуров А.Е., Жумажанов Б.Р., Дайнеко Е.А., Зылғара А.Е.
Алгоритм определения начальных орбитальных параметров KazEOSat-1
для деорбитации.....236

**Мименбаева А.Б., Туребаева А.Д., Оспанова Т.Т., Аруова А.Б.,
Найзағараева А.А.**
Разработка и сравнительный анализ моделей машинного обучения
для прогнозирования городского трафика.....253

Науменко В.В., Муканова Ж.А., Киселёва О.В., Майнцер Д.А., Нерезов А.К.
Применение опросов в режиме реального времени для повышения
успеваемости обучающихся.....271

Назырова А.Е., Кадеркеева З.К., Бекманова Г.Т., Милош М., Ламашева Ж.Б.
Цифровое образование и академическая успеваемость учащихся:
межуровневый анализ.....287

Оралбекова Д., Мамырбаев О., Ахмедиярова А., Касымова Д., Алибиева Ж.
Разработка многоуровневой модели для абстрактивного резюмирования текста
на основе предварительно обученных моделей.....316

**Оразбаев Б.Б., Жумадиллаева А.К., Курбангалиева Н.Б., Есиркесинов Р.Ж.,
Оразбаева К.Н.**
Синтез лингвистических моделей оценки качества серы и нечёткое
моделирование процесса её производства.....337

Сарсенбаева А.К., Рахимова Д.Р., Шормакова А.Н., Мансурова М.Е., Адали Э.
Применение семантических методов в юридическом анализе: интеллектуальная
система для обработки агглютинативных текстов.....354

Серек А., Шойынбек А., Шарипов К., Куанышбай Д., Мухаметжанов А.
Анализ и классификация телефонного мошенничества на основе
лексических признаков речевых транскрипций.....373

Шынжігіт Б.Б., Балабекова М.О., Амангелді Т.Т.
Анализ и прогнозирование объёмов продаж кирпичной продукции
с использованием машинного обучения.....393

Тохаева А.О., Альжанов А.К., Nezih Ö., Зиятбекова Г.З., Бегалиева К.Б.
Формирование компетенций в области виртуализации у обучающихся
в высшем образовании на основе платформы Proxmox VE.....412

Тукенова Л.М., Ауелбеков О.А., Сапакова С.З., Саметова А.А., Бостанов Е.Л.
Моделирование и оптимизация режимов работы гибридных силовых установок
для беспилотных летательных аппаратов.....430

Еримбетова А.С., Бержанова У.Г., Дайырбаева Э.Н., Сакенов Б.Е., Самбетбаева М.А.
Распознавание языка жестов с использованием временных свёрточных
сетей и MediaPipe4.....43

Жукабаева Т.К., Бенхелифа Э., Марденов Е.М., Баумуратова Д., Карабаев Н.
Поддержка принятия решений при реагировании на атаки в киберфизических
промышленных системах интернета вещей.....461

ACADEMIC SCIENTIFIC JOURNAL OF COMPUTER SCIENCE
ISSN 1991-346X
Volume 1.
Namber 357 (2026). 167–181

https://doi.org/10.32014/2026.2518-1726.407

IRSTI: 28.23.01
UDC 004.855

© Dzhsupbekova G.[1], Othman M.[2], Ordabayeva G. [3,4*], 2026.

[1]M. Auezov South Kazakhstan State University, Shymkent, Kazakhstan;
[2]Universiti Putra Malaysia, Selangor D.E., Malaysia;
[3]Bolashak Program, Scientific internship, UC Davis, USA;
[4]Kazakh National University named after Al-Farabi, Almaty, Kazakhstan.
E-mail: gordabayeva@ucdavis.edu

COMPARATIVE ANALYSIS OF ARTIFICIAL INTELLIGENCE ALGORITHMS TO DETECT NETWORK ATTACKS

Dzhsupbekova Gulzat — Candidate of Pedagogical Sciences, Head of the Department of Information Technology, M. Auezov South Kazakhstan State University, Shymkent, Kazakhstan,
E-mail: gulzat20.10@mail.ru, ORCID ID: https://orcid.org/0000-0003-1727-0966;
Mohamed Othman — Professor, Department of Communication Technology and Networks, Universiti Putra Malaysia, Serdang, Malaysia,
E-mail: mothman@upm.edu.my, ORCID ID: https://orcid.org/0000-0002-5124-5759;
Ordabayeva Gulzinat — Bolashak Program, Scientific internship, UC Davis, USA; Senior lecturer at the Department of Cybersecurity and Cryptology, Kazakh National University named after Al-Farabi, Almaty, Kazakhstan,
E-mail: gordabayeva@ucdavis.edu, ORCID ID: https://orcid.org/0000-0001-9952-1620;

Abstarct. The rapid development of information technologies and the expansion of digitalization trends have a huge impact on all spheres of life of society and the economy. The complication of network infrastructures and the sharp increase in the number of devices connected to the internet have increased the volume of information flow, as well as created new security challenges. The types and methods of cyberattacks are changing rapidly, and traditional methods of protection, as before, are often insufficient. Large enterprises are using artificial intelligence (AI) systems that can independently learn patterns and analyze complex data streams instead of traditional rule-based systems. These methods allow you to detect attacks faster and more accurately because they can quickly detect patterns and anomalies. The purpose of the article is to conduct a comparative analysis based on deep learning methods to accurately and quickly identify threats in network traffic and prove its effectiveness in practice. To analyze the potential of machine learning (ML) and deep learning (DL) methods, traditional algorithms such as Random

Forest, XGBoost, and SVM were employed together with a convolutional neural network (CNN) architecture. Model training was conducted in Python using the CIC-IDS-2017 dataset. The data were stored in * parquet format and underwent preprocessing, including the removal of missing values, scaling of numerical features, and encoding of categorical variables. Attack types were encoded using predefined labels, and scaling was performed using StandardScaler. The dataset was split into 70% for training and 30% for testing. Artificial intelligence algorithms have been relatively analyzed in terms of classifying attack types, distinguishing between normal and abnormal traffic, as well as detecting new or rare attacks. As a result of the study, indicators of accuracy, sensitivity, F1-score, ROC-AUC curve and error matrix were evaluated. In addition, the real-time application of the proposed methods and their practical significance were analyzed.

Keywords: network attack, artificial intelligence, deep learning, machine learning, neural network, types of attacks, comparative analysis

For citations: Dzhsupbekova G., Othman M., Ordabayeva G. Comparative analysis of artificial intelligence algorithms to detect network attacks. Academic Scientific Journal of Computer Science, 2026. — No.1. – P. 167–181. DOI: https://doi.org/10.32014/2026.2518-1726.407

© Джусупбекова Г.[1], Othman M.[2], Ордабаева Г.[3,4*], 2026.
[1]М. Ауэзов атындағы Оңтүстік Қазақстан университеті,
Шымкент, Қазақстан;
[2]Putra университеті, Selangor D.E., Малайзия;
[3]«Болашақ» бағдарламасы, ғылыми тағылымдама, UC Davis, USA;
[4]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан.
E-mail: gordabayeva@ucdavis.edu

ЖАСАНДЫ ИНТЕЛЛЕКТ АЛГОРИТМДЕРІН ЖЕЛІЛІК ШАБУЫЛДАРДЫ АНЫҚТАУ ҮШІН САЛЫСТЫРМАЛЫ ТАЛДАУ

Джусупбекова Гулзат — педагогика ғылымдарының кандидаты, «Ақпараттық-коммуникациялық технологиялар» кафедрасының меңгерушісі, М. Ауэзов атындағы Оңтүстік Қазақстан университеті, Шымкент, Қазақстан,
E-mail: gulzat20.10@mail.ru, ORCID ID: https://orcid.org/0000-0003-1727-0966;
Mohamed Othman — Communication Technology and Networks кафедрасының профессоры, Putra университеті, Серданг, Малайзия,
E-mail: mothman@upm.edu.my, ORCID ID: https://orcid.org/0000-0002-5124-5759;
Ordabayeva Gulzinat — "Болашак" бағдарламасы, ғылыми тағылымдама, UC Davis, USA; «Киберқауіпсіздік және криптология» кафедрасының аға оқытушысы, әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан,
E-mail: gordabayeva@ucdavis.edu, ORCID ID: https://orcid.org/0000-0001-9952-1620.

Аннотация. Қазіргі кезеңде ақпараттық технологиялардың жедел дамуы және цифрландыру үрдістерісінің кең таралуы қоғамның, экономиканың және адам өмірінің көптеген салаларына елеулі ықпал етуде. Желілік инфрақұрылымдардың күрделене түсуі және интернетке қосылған құрылғылар санының қарқынды өсуі ақпараттық ағын көлемінің ұлғаюына әкеліп қана қоймай, сонымен қатар ақпараттық қауіпсіздік саласында жаңа қауіп-қатерлердің пайда болуына себеп болды. Кибершабуылдардың түрлері мен жүзеге асыру әдістері үнемі өзгеріп, жетілдіріліп отырғандықтан, дәстүрлі қорғаныс тәсілдері қазіргі сәтте көптеген жағдайларда жеткіліксіз болып отыр. Бүгінде ірі ұйымдарда дәстүрлі ережелерге негізделген жүйелердің орнына деректерден заңдылықтар мен үлгілерді өздігінен үйрене алатын және күрделі ақпараттық ағындарды талдайтын жасанды интеллект (AI) технологиялары кеңінен қолданылуда. Мұндай тәсілдер кибершабуылдарды неғұрлым жылдам әрі дәл анықтауға мүмкіндік береді, өйткені олар деректердегі жасырын үлгілер мен аномалияларды тиімді түрде айқындай алады. Бұл мақаланың мақсаты – желілік трафиктегі қауіп-қатерлерді дәл әрі жедел анықтауға бағытталған терең оқыту әдістеріне негізделген модельдеоге салыстырмалы талдау жасап, олардың тиімділігін тәжірибелік зерттеу нәтижелері арқылы көрсету. Зерттеу барысында жасанды интеллект негізіндегі бірнеше әдіс сыналды. Машиналық оқыту (МО) және терең оқыту (Deep Learning) алгоритмдерінің мүмкіндіктері зерттеле отырып, Random Forest, XGBoost, SVM сияқты дәстүрлі әдістермен қатар нейрондық желілердің заманауи архитектурасы – CNN қолданылды. Барлық модельдер CIC-IDS-2017 деректер қорын қолдана отырып Python негізінде үйретілді. Ақпараттар *.parquet форматында сақталынды және алдын ала өңделді, яғни бос мәндер жойылды, сандық шкалаға келтірілді, категориялар кодталды. Шабуыл түрлері сандық кодтау арқылы белгіленіп, деректер StandardScaler көмегімен масштабталды. Деректер жиыны 70% оқу және 30% тестілеу бөліктеріне бөлінді. Жасанды интеллект алгоритмдері шабуылдарды жіктеу, қалыпты және аномальды трафикті анықтау, сондай-ақ жаңа немесе сирек шабуылдарды табу қабілеті бойынша салыстырмалы түрде бағаланды. Зерттеу нәтижесінде дәлдік, сезімталдық, F1-score, ROC-AUC қисығы және қателік матрицасы көрсеткіштері бағаланды. Бұдан бөлек, ұсынылған әдістердің нақты уақыт режимінде қолданылу мүмкіндіктері мен олардың практикалық тиімділігіне талдау жүргізілді.

Түйін сөздер: желі шабуылы, жасанды интеллект, терең оқыту, машиналық оқыту, нейрондық желі, шабуыл түрі, салыстырмалы талдаулар

©Джусупбекова Г.[1], Othman M.[2], Ордабаева Г.[3,4*], 2026.
[1]Южно-Казахстанский университет имени М. Ауэзова, Шымкент, Казахстан;
[2]Университет Putra, Selangor D.E., Малайзия;
[3]Программа «Болашак», научная стажировка, UC Davis, USA;
[4]Казахский Национальный университет имени ал-Фараби,
Алматы, Казахстан.
E-mail: gordabayeva@ucdavis.edu

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

Джусупбекова Гулзат – кандидат педагогических наук, зав. кафедрой «Информационно-коммуникационные технологии», Южно-Казахстанский университет имени М. Ауэзова, Шымкент, Казахстан,
E-mail: gulzat20.10@mail.ru, ORCID ID: https://orcid.org/0000-0003-1727-0966;
Mohamed Othman – профессор кафедры Communication Technology and Networks, Университет Putra, Серданг, Малайзия,
E-mail: mothman@upm.edu.my, ORCID ID: https://orcid.org/0000-0002-5124-5759;
O**rdabayeva Gulzina**t – Программа “Болашак”, научная стажировка, UC Davis, USA; ст.преп. кафедры «Кибербезопасность и криптология», Казахский национальный университет имени аль-Фараби, Алматы, Казахстан,
E-mail: gordabayeva@ucdavis.edu, ORCID ID: https://orcid.org/0000-0001-9952-1620.

Аннотация. Стремительное развитие информационных технологий и расширение процессов цифровизации оказывают значительное влияние на все сферы жизни общества и экономики. Усложнение сетевой инфраструктуры и рост числа устройств, подключённых к сети Интернет, приводят к увеличению объёма трафика и появлению новых угроз информационной безопасности. В современных условиях в крупных организациях всё шире применяются системы искусственного интеллекта (ИИ), способные автоматически выявлять закономерности и анализировать сложные потоки данных. Такие методы обеспечивают более быстрое и точное обнаружение атак за счёт выявления скрытых зависимостей и аномалий в сетевом трафике. Целью исследования является сравнительный анализ методов машинного и глубокого обучения, направленных на эффективное выявление сетевых атак, а также экспериментальная оценка их результативности. В работе рассмотрены как классические алгоритмы машинного обучения (Random Forest, XGBoost, SVM), так и современные нейросетевые архитектуры, включая сверточные нейронные сети (CNN). Модели обучались с использованием языка программирования Python на основе набора данных CIC-IDS-2017. Предварительная обработка данных включала удаление пропущенных значений, масштабирование числовых признаков с использованием StandardScaler, кодирование категориальных переменных, а также преобразование данных в формат *.parquet. Данные

были разделены на обучающую и тестовую выборки в соотношении 70% и 30% соответственно. Сравнительный анализ алгоритмов проводился по ряду критериев, включая точность классификации, способность различать нормальный и аномальный трафик, а также выявление редких и ранее неизвестных атак. В качестве метрик оценки использовались accuracy, recall (чувствительность), F1-score, ROC-AUC и матрица ошибок. Результаты исследования показали, что методы глубокого обучения демонстрируют более высокую эффективность при выявлении сложных паттернов сетевых атак, в то время как классические алгоритмы обеспечивают устойчивые результаты при меньших вычислительных затратах.

Ключевые слова: сетевая атака, искусственный интеллект, глубокое обучение, машинное обучение, нейронная сеть, типы атак, сравнительный анализ

Кіріспе. Желілік шабуыл – ұйымның ақпараттық желісіне рұқсатсыз кіру арқылы деректерді заңсыз алу немесе зиян келтіру мақсатындағы әрекет. Желілік шабуылдардың ең жиі кездесетін түрлері – пассивті және белсенді шабуылдар. Пассивті шабуыл кезінде шабуылдаушы желі трафигін тыңдап немесе ақпаратты ұрлап алады, бірақ деректерді өзгертпейді, яғни олардың бастапқы күйін сақтайды. Белсенді шабуылдарда рұқсатсыз қатысушылар жүйеге заңсыз кіріп, деректерді жоюға, шифрлауға немесе бүлдіруге мүмкіндік алады.

Кең таралған желілік шабуылдар сипаттамалары:

- Таратылған қызмет көрсетуден бас тарту (Distributed Denial of Service, DDoS) шабуылдары. Зиянкестер ботнеттерді – басқараылатын зиянды құрылдғылар желісін қолданып серверлерге немесе желілерге жалған трафик жібереді. DDoS-шабуылдар желілік деңгейде (серверді шамадан тыс жүктейтін SYN/ACK пакеттерінің легі) немесе қолданбалы деңгейде (дерекқорларды бұзуға бағытталған күрделі SQL-сұраныстар арқылы) жүзеге асыруы мүмкін (Aljabri et al., 2021; Singh et al., 2022).

- MITM (Man-In-The-Middle) шабуылдарды зерттеулерде (Salem et al., 2022) IoMT жүйелерінде қашықтан денсаулық мониторингін бұзудан қорғау және шабуылдардың ықпалын төмендету жолдару ретінде талданған. Деректердің құпиялылығын қамтамасыз ету үшін физиологиялық көрсеткіштер орнына LSH-қолтаңбасы енгізілді, ал олардың тұтастығын сақтау мақсатында RSSI мәніне негізделген HMAC кілті қолданылды.

- Кодтық және SQL инъекция шабуылдары. Көптеген веб-сайттар пайдаланушы енгізген деректерді өңдейді, алайда оларды дұрыс тексеріп, зарарсыздандырмауы мүмкін. Осы жағдайларда зиянкестер веб-формалар мен API сұраныстарын пайдалана отырып, жүйеге зиянды код енгізуге қабілетті. Осы код серверде іске қосылған жағдайда жүйенің осалдықтарын пайдаланып, дерекқорға кіруге немесе оны басқаруға мүмкіндік береді (Tadhani et al., 2024.

- Артықшылықтарды кеңейту (Privilege Escalation) кезінде шабуылдаушы-

лар желіге кіргеннен соң өз мүмкіндіктерін арттыру мақсатында сәйкес әдістерді қолданады. (Muslam, 2023) зерттеуінде инсайдерлік шабуылдарды анықтау және жіктеу үшін машиналық оқыту алгоритмдерін ұсынады және талдауда бірнеше Cert деректер жиынтығы қолданылды.

- Ішкі қауіптер (Insider Threats) – ұйымдағы артықшылықты рұқсаттарға ие қызметкерлер тарапынан туындайтын қауіптер, олар желілік инфрақұрылымның осалдығын арттыра алады. (Ye et al., 2025) өз зерттеулерінде Cert деректер жиынтығын конвульсиялық нейрондық желі (CNN) негізінде инновациялық архитектура ұсынды. Зерттеу нәтижелері көрсеткендей, бұл тәсіл корпоративтік ортада инсайдерлік қауіптерді анықтаудың дәлдігі мен сенімділігін елеулі түрде жақсартады.

Материалдар мен әдістер. Қазіргі уақытта МО алгоритмдері үлкен деректер жиынтығын өңдеп, ықтимал қауіптерді көрсететін үлгілер мен аномалияларды анықтауға, сондай-ақ күрделі кибершабуылдарды тануға қабілетті.

МО алгоритмдеріне негізделген жүйелер деректерді нақты уақыт режимінде өңдеуге мүмкіндік беріп, киберқауіптерді жылдам анықтау және оларға оперативті жауап беру арқылы кибершабуылдардың ықтимал зиянын төмендетуге ықпал етеді.

Машиналық оқытуға негізделген мінез-құлықты терең талдау пайдаланушының қалыпты белсенділік үлгілерін тиімді анықтауға мүмкіндік береді. Қалыпты әрекет үлгілерінен кез келген ауытқулар қауіпсіздікке қатер төндіруінің ықтимал белгісі ретінде қарастырылады, бұл зиянды әрекеттерді ерте анықтап, алдын алу мүмкіндігін қамтамасыз етеді. Болжамдық талдау әдістері өткен деректерді талдай отырып, МО арқылы ықтимал болашақ қауіптер мен жүйелік осалдықтарды алдын ала болжауға мүмкіндік береді. Бұл белсенді қорғаныс әдістері ұйымдарға шабуылдардың алдын алу мақсатында қауіпсіздік шараларын алдын ала күшейтуге мүмкіндік береді (Zou, 2025).

Әдеби шолу

ЖИ даму кезеңдері

ЖИ әдістері желілік шабуылдарды алдын ала анықтау және олардың нақты классификациясын жүргізуге мүмкіндік береді. Бұл тәсілдер шабуылдардың индикаторларын ерте тануға және оларға жылдам әрі тиімді түрде әрекет етуге мүмкіндік береді.

ЖИ алгоритмдері МО әдістерін пайдаланып желідегі әрекет үлгілерін меңгеріп, жаңа қауіп-қатерлерге тиімді бейімделуге қабілетті. ЖИ жүйелері инциденттерге автоматты түрде әрекет ете отырып, киберқауіптерді басқаруда мамандардың уақытын тиімді пайдалануға жағдай эжасайды.

ЖИ эволюциясы және киберқауіпсіздікке ықпалы:

1. Алғашқы кезең (1900-1950 жж.) – ережеге негізделген жүйелердің дамуы.

2. Өтпелі кезең (1950–1980 жж.). Статистикалық әдістер және алғашқы МО модельдері..

3. Қалыптасу кезеңі (1980-2020 жж.) – үлкен деректер және МО модельдерінің жетілу кезеңі.

4. Қазіргі кезең (2021 – қазіргі уақытқа дейін) – терең оқыту және өзіндік үйрену қабілеті бар жүйелердің қалыптасуы мен жетілдірілуі.

Киберқауіпсіздік саласында терең оқыту (көпқабатты нейрондық желілер) кеңінен қолданылады. Өздігінен үйренетін ЖИ жүйелері, мысалы, Darktrace және Vectra AI, нақты уақытта желідегі әрекеттерді талдап, шабуылдарды автоматты түрде анықтайды. Сонымен қатар, бұл технологиялар бұлттық қауіпсіздік, IoT құрылғыларды қорғау, блокчейн қауіпсіздігі және API трафигін бақылау сияқты жаңа бағыттарды дамытуға мүмкіндік береді (Asambaev, 2011; Mucci, 2024; Muthukrishnan, 2020).

Классикалық IDS/IPS жүйелері сигнатураларға негізделгендіктен, жаңа немесе белгісіз шабуылдарды тиімді анықтай алмайды. Бұл кемшілікті ЖИ негізіндегі жүйелер жоя алады. ЖИ технологиялары шабуылдарда тануда келесі әдістерді қолдануға мүмкіндік береді:

1. Зиянды трафикті анықтау – ЖИ алгоритмдері желілік трафикті автоматты түрде талдай отырып, қалыпты және зиянды мінез-құлық үлгілерін тиімді ажырата алады. Терең нейрондық желілер (DNN) және рекуренттік нейрондық желілер (RNN) желілік сессиялардағы уақыттық заңдылықтарды идентификациялауға арналған. NSL-KDD немесе CICIDS2017 секілді датасеттерді пайдалана отырып, ЖИ жүйесі шабуылдарды (DoS, Probe, R2L, U2R) нақты ажырата алады. Мұнда әрбір пакет немесе байланыс сеансы белгіленген сипаттамалар (features) бойынша өңделеді.

2. Аномалияларды анықтау – ЖИ көмегімен "қалыптыдан ауытқыған" әрекеттерді табу. Мұнда бақылаусыз оқыту (unsupervised learning) әдістері, K-means, DBSCAN, Autoencoder кеңінен қолданылады. Бұл әдіс жаңа шабуыл түрлерін анықтауға мүмкіндік береді, себебі олар әлі белгілі шаблондарға сәйкес келмеуі мүмкін.

3. Кластерлеу және жіктеу - ЖИ шабуылдарды түрлеріне қарай жіктеу үшін SVM, CNN, Random Forest сияқты алгоритмдерді қолданады. Алдын ала оқытылған үлгілер негізінде жүйелер трафиктің зиянды немесе қалыпты екенін анықтайды.

4. DDoS шабуылдарын ерте анықтауда ЖИ пакеттер ағынын нақты уақыт режимінде талдай отырып, шабуылдың бастапқы белгілерін анықтай алады. LSTMсияқты терең оқыту модельдері уақытша тәуелділіктерді зерттеу арқылы шабуыл басталмай тұрып есекерту сигналдарын береді (Zhunisov, 2024).

ЖИ модельдерін оқытуда қолданылатын дереккөздер

Желілік шабуылдарды анықтауға арналған ЖИ жүйелерін тиімді үйрету үшін нақты және репрезентативті деректер жиынтықтары қажет. Қазіргі зерттеулерде кеңінен қолданылатын деректер жиынтықтарына мыналар жатады:

- KDD Cup 99 – классикалық кибершабуылдарды қамтитын деректер;

- NSL-KDD – KDD Cup 99 деректер жиынтығының жетілдірілген және жаңартылған нұсқасы;

- CSE-CIC-IDS2017 – заманауи шабуыл түрлерін және толық метаақпаратты қамтитын деректер жиынтығы;

- UNSW-NB15 – қалыпты және зиянды трафиктің теңгерімді үлгілерін қамтитын деректер жиынтығы.

Зерттеуде негізгі дереккөз ретінде желілік шабуылдарды анықтауда жиі қолданылатын CIC-IDS-2017 таңдалды. Бұл дерекқор құрамында зертханалық ортада құрастырылған нақты желі трафигі және қалыпты белсенділігі бар түрлі шабуылдар бар. Мәліметтер flow-based features типтес желі легімен берілген. Мұнда қосылу ұзақтығы, пакеттер саны, байт сипаттамалары және уақыт параметрлері сияқты желілік өзара әрекеттесудің статистикалық сипаттамасы бар. Деректер қоры құрамында бірнеше кластар бар және деректер көп кластық бойынша жіктеледі: Benign (қалыпты трафик), DDoS, DoS (Hulk, GoldenEye, Sloworis, Slowhttptest), PortScan, Bot, FTP-Patator, SSH-Patator, Web Attack (Brute Forse, XSS), Infiltration.

Аталған деректер жиынтықтары негізінде ЖИ модельдерін оқытып, оларды нақты желілік шабуылдарды тануға үйретуге болады. ЖИ жүйелерінің жұмыс тиімділігін бағалау үшін келесі негізгі метрикалар қолданылады:

- Accuracy – дұрыс классификацияланған жағдайлардың жалпы үлесі;
- Precision – шабуыл ретінде анықталған әрекеттердің ішінде нақты шабуыл болғандарының үлесі;
- Recall (Sensitivity) – барлық нақты шабуылдардың ішінде жүйе дұрыс анықталғандарының үлесі;
- F1-score – precision және recall көрсеткіштерінің гармониялық орташа мәні (Khan et al., 2021).

ЖИ әлемдік компанияларда қолданылуы

1. Google компаниясының Gmail қызметіндегі фишингтік шабуылдарды анықтау мақсатында ЖИ және МО алгоритмдері кеңінен қолданылады. Мысалы, Gmail жүйесі әрбір кіріс хатты жүздеген параметр бойынша талдайды, оның ішінде мәтін құрылымы, тақырып мазмұны, сілтемелердің сипаты, IP мекенжай мәліметтері және басқа сипаттамалар бар. Осындай талдау нәтижесінде жүйе күн сайын 100 миллионнан астам фишингтік хабарламаны автоматты түрде бұғаттай алады (Google AI Blog, 2023).

2. IBM компаниясы дамытқан QRadar жүйесі ақпараттық қауіпсіздік орталықтарында (Security Operation Center, SOC) кеңінен қолданылады. Аталған жүйе ЖИ технологияларын пайдалана отырып, желідегі аномалияларды, рұқсатмыз әрекеттерді және ықтимал шабуылдарды нақты уақыт режимінде анықтайды (IBM Security, 2022).

3. Darktrace - Ұлыбританияда құрылған киберқауіпсіздік саласындағы компания. Ол желілік шабуылдарды анықтау үшін ЖИ негізделген өзіндік оқытылатын жүйені пайдаланады. Аталған жүйе ұйымның ішкі желісіндегі қалыпты әрекеттерді талдап, олардан ауытқыған кез келген аномалды белсенділікті ықтимал қауіп ретінде анықтап, жедел хабарлама жібереді. Darktrace технологиялары әлемнің 100-ден астам елінде қолданылып, қаржы, денсаулық сақтау және өндіріс секторларында кеңінен енгізілген (Darktrace, 2025).

4. Kaspersky компаниясы зиянды бағдарламалардың жаңа түрлерін анықтау мақсатында DL және үлгіге негізделген (pattern-based) талдау әдістерін пайдаланады. Бұл тәсіл компанияға жыл сайын миллиондаған жаңа кибершабуыл түрлерін автоматты түрде анықтап, оларды жоюға мүмкіндік береді (Kaspersky, 2024).

5. Қазақстан Республикасында 2017 жылдан бастап жүзеге асырылып келе жатқан «Киберқалқан» бағдарламасы аясында ақпараттық қауіпсіздік жүйелеріне жасанды интеллект енгізілуде. Аталған жүйелер мемлекеттік органдар мен ұлттық инфрақұрылымды кибершабуылдардан қорғау мақсатында желілік трафикті үздіксіз мониторингтен өткізіп, шабуылға тән аномалияларды автоматты түрде анықтайды. Нәтижесінде жүйе мемлекеттік деректер базаларына бағытталған шабуыл әрекеттерінің алдын алуға мүмкіндік береді (Киберқалқан, 2025).

Нәтижелер

Модельді бағалаудағы классификация метрикалары

ЖИ модельдерін желілік шабуылдарды анықтау және жіктеу үшін қолданғанда, ең басты міндет – модельдің тиімділігін дәл бағалау. Нақты уақытта қолданылатын модель тек болжам жасап қана қоймай, сол болжамның сенімді және қауіпсіз екенін де қамтамасыз етуі қажет.

ЖИ мен МО әдістері негізінде құрылған желілік шабуылдарды анықтау модельдерінің сапасын дұрыс бағалау – жүйенің сенімділігі мен тиімділігін қамтамасыз етудің негізгі құрамдас бөлігі. Бағалау критерийлері мен метрикалар шабуылдарды нақты және толық анықтауға мүмкіндік беріп қана қоймай, сонымен қатар жалған позитивтер (false positives) мен жалған негативтерді (false negatives) де өлшеуге мүмкіндік береді.

Көбінесе модельді бағалауда бинарлық классификация метрикалары қолданылады, себебі көптеген жүйелер қалыпты және шабуыл трафигін ажыратуға бағытталған. Егер шабуылдардың түрлерін бөлу қажет болса, көпкласты классификация метрикалары да қолданылады, атап айтқанда:

1. CIC-IDS-2017 деректер қорындағы кластарды талдау (1-кесте).

1 кесте – Қалыпты трафиктің және шабуыл түрлерінің саны (CIC-IDS-2017 дерек қоры)

Р/н	Класс атауы	Саны
1	Benign	2273097
2	DoS Hulk	231073
3	PortScan	158930
4	DDoS	128027

5	DoS GoldenEye	10293
6	FTP-Patator	7938
7	SSH-Patator	5897
8	DoS Sloworis	5796
9	DoS Slowhttptest	5499
10	Bot	1966
11	Web Attack Brute Forse	1507
12	Web Attack XSS	652
13	Infiltration	36

Қарастырылған деректер қорында басым көпшілікті Benigh класы құрайды. Сонымен қатар, ең төменгі мәлімет Infiltration класына тиесілі. Бұл теңгерімсіздік МО модельдерін құру кезінде ескерілген.

2. Дәлдік (Accuracy) – модельдің барлық болжамдар ішінде дұрыс болжам жасаған жағдайларының үлесін сипаттайтын метрика (1):

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

Дәлдік (Accuracy) тек теңгерілген (balanced) деректерде ғана толық ақпарат береді. Егер шабуылдардың саны аз болса, модель барлық трафикті «қалыпты» деп бағалап, жоғары дәлдік көрсеткіші алуы мүмкін. Алайда бұл жағдай модельдің шынайы тиімділігін көрсетпейді, себебі нақты шабуылдарды анықтау қабілеті төмен болады.

3. Нақтылық (Precision) – модельдің шабуыл деп белгіленген трафигінің ішінде шынайы шабуылдардың үлесін көрсететін метрика (2):

$$\text{Precision} = \frac{TP}{TP+FP} \quad (2)$$

Егер модель көп мөлшерде FP (жалған оң) жағдайлар тудырса, жүйеге сенім төмендейді. Сол себепті нақтылық (Precision) маңызды метрика болып табылады, себебі ол модельдің қате ескертулерін бағалауға мүмкіндік береді.

4. Recall немесе Detection Rate - модель нақты шабуылдардың қаншасын дұрыс анықтағанын көрсетеді (3).

$$\text{Recall} = \frac{TP}{TP+FN} \quad (3)$$

Бұл көрсеткіш әсіресе қауіпсіздік саласында аса маңызды,өйткені FN (жіберіп алған шабуылдар) жүйеге үлкен зиян келтіруі мүмкін.

5. F1-score - нақтылық пен сезімталдықтың үйлесімі, екі метриканың арасындағы тепе-теңдікті көрсетеді (4).

$$\text{F1-score} = 2 \cdot \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (4)$$

F1-score теңгерімсіз деректерде (шабуыл үлесі 10%-дан аз) өте маңызды. Ол модельдің жалпы тиімділігін жақсы сипаттайды.

Берілген формулалар негізінде тұрғызылған МО модельдерін талдау 2 кестеде берілген.

2 кесте – МО модельдерін салыстыру

Модель атауы	Accuracy	Precision	Recall	F1-Score
CNN	0.953111	0.950174	0.953111	0.949316
Random Forest	0.995111	0.994960	0.995111	0.994887
SVM	0.945778	0.943968	0.945778	0.942091

Жалпы алғанда, Random Forest алгоритмі салыстырмалы талдауда жоғары көрсеткішке ие болды.

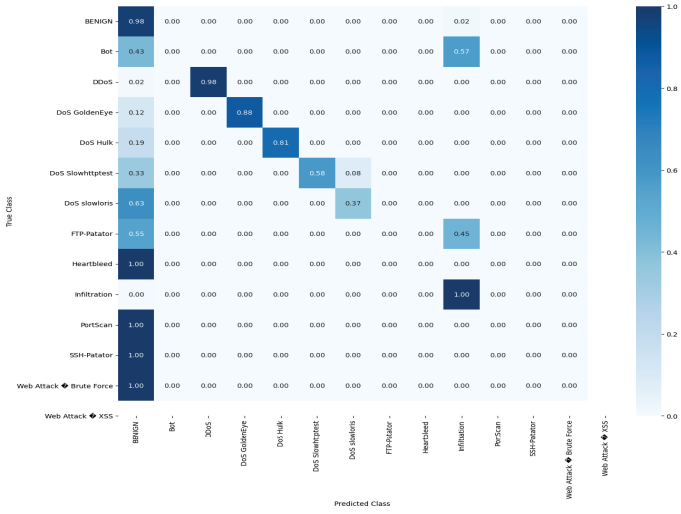
Модельдерді оқыту алгоритмдерін салыстырмалы талдау

Келесі МО және DL модельдеріне салыстырмалы талдау жүргізілді:

- Random Forest – ансамльдік ағаштар әдісі;
- SVM – қолдау векторлар машиналары;
- CNN – конволюциялық нейрондық желі.

Барлық модельдер CIC-IDS-2017 датасеті негізінде үйретілді. Мәліметтер MachineLearningCSV.csv форматында сақталып, алдын ала өңделді (бос мәндер жойылды, сандық шкалаға келтірілді, категориялар кодталды). Шабуыл түрлері сандық кодтау арқылы көрсетілді, ал ерекшеліктер StandardScaler негізінде масштабталды. Деректер оқыту және тест жиынтығына бөлінген, мұнда оқыту жиынтығы деректердің 70% , ал тест жиынтығы 30% қамтиды.

Кластар бойынша қателік матрицасы CNN алгоритмінің тест деректерінде әр шабуыл класын қаншалықты дұрыс немесе бұрыс анықтағанын көрсетеді (2 - сурет).



2 сурет – Кластар бойынша қателік матрицасы

Қателік матрицасының нәтижелеріне сүйенсек, CNN моделі желілік шабуылдарды жіктеуде жоғары тиімділік көрсетті. Талдау көрсеткендей Benign, DoS Hulk, DDoS Portscan кластары жоғары дәлдікті көрсететті, мұнда диагональдағы мәндер 0,85-0,98 деңгейінде болады. Сонымен қатар, кейбір кластар үшін жіктеу қателері бар. Графикте Bot класы Benign және басқа шабуылдаушы сыныптармен шатастырылады. Сол сияқты, DoS Slowloris және DoS Slowhttptest кластары өзара қателіктерді көрсетеді. Жалпы модель қалыпты желілік трафикті сенімді түрде ажырата алатыны көрсетілді.

Талқылау

(AL-Jaberi et al., 2025) зерттеулерінде МО алгоритмдеріне арналған жаңа мұздату әдісі ұсынылды және пирамида сұлбасын пайдалана отырып, фишингтік веб-сайттарды анықтаудың жетілдірілген тәсілі жасалды. Жаңа модель ең маңызды белгілерге назар аударып, фишинг сайттарды дәл анықтауды қамтамасыз етеді және қайта оқытуды қажет етпейді. Ұсынылған модельде 30 атрибуты бар 2456 ақпараттан тұратын деректер қоры негізінде Random Forest алгоритмі фишингтік сайттарды анықтауды 97,4% дәлдікте көрсетті.

(Cárdenas-Haro et. al., 2025) өз зерттеулерін Sybil шабуылына қатысты әдеби шолудан бастаған. Мақалада Sybil шабуылына осал желілер қауіпсіздігін қамтамасыз етудегі қорғаныс шаралары және шабуылдың алдын-алу алгоритмдері қарастырылған. Онлайн әлеуметтік желілерде, соның ішінде Twitter-де Sybil байланысын анықтау алгоритмі зерттеудің негізі болып табылады. Sybil шабуылын KNN алгоритмі 96% - 97%, *SVM* алгоритмінің көрсеткіші 97% - 100% дәлдікпен анықтады. Зерттеуде қорғаныс шараларын қолданудың қадамдары, нәтижелерді талдау және болашақтағы зерттеу бағыттары баяндалған.

(Kuraś et.al., 2026) зерттеуінде IoT-құрылғыларындағы шектеулі ресурстар жағдайында желі трафигіндегі аномальды әсерді бақылау мақсатында МО модельдерін оңтайландыруды қарастыра отырып RandomForest, ExtraTrees, AdaBoost, XGBoost, CatBoost алгоритмдеріне салыстырмалы талдау жасалған. Қорытынды да XGBoost алгоритмі бинарлы классификация негізінде 92% дәлдікпен 8 секунд арасында МО оңтайлы моделі екенін көрсетті.

(Altwaijry et al., 2024) зерттеулерінде фишингтік электрондық пошта хабарларын анықтау үшін бірөлшемді конволюциялық нейрондық желілерге (1D-CNNPD) негізделген модельдер қолданылды. Базалық 1D-CNNPD модель рекуренттік қабаттармен – LSTM, Bi-LSTM, GRU және Bi-GRU – күшейтілгенде оның анықтау дәлдігі артатыны дәлелденген. Зерттеу барысында фишингті анықтауға арналған конволюциялық нейрондық желі (CNN) негізіндегі 12 DL моделі ұсынылған. Талдау нәтижесінде Leaky ReLU және Bi- GRU моделінің негізінде өнімділік көрсеткіштері Acc.99.68%, F1 99.66% тең болды. Бұл көрсеткіш 1D-CNNPD моделінің электрондық пошта арқылы фишингтік шабуылдармен күресу үшін киберқауіпсіздік шешімдерін іске асырудағы әлеуетін көрсетеді.

(Bolatbek et. al., 2024) зерттеулерінде деструктивті хабарламалардың таралуын YouTube, Vkontakte және Telegram сияқты әлеуметтік желілерден ақпарат жинау арқылы қарастырған. Мақалада e uni-bi-gram(1,2) көмегімен Logistic Regression, SVM, Naive Bayes әдістерінен алынған нәтижелердің жиынтығы көрсетілген. Сонымен қатар, фишингтік веб-сайттарды анықтау, желі қауіпсіздігін қамтамасыз ету және шабуылдарды алдын алу, сондай-ақ әлеуметтік желілердегі деструктивті хабарламалардың таралуын болжау үшін МО модельдері мен DL алгоритмдері қарастырылған.

Біздің зерттеуімізде желілік шабуылдарды анықтауда CNN моделі негізіндегі көрсеткіш 98,13% дәлдікпен дұрыс анықтады.

(Altwaijry et. al., 2024) зерттеуінде LSTM, Bi-LSTM, GRU және Bi-GRU қабаттарымен кеңейтілген кездегі өнімділік көрсеткіштері 99.68%, ал біз қарастырған Random Forest, XGBoost, SVM орташа нәтижелері 98%, яғни бұл тұрғызылған модель сенімділігінің жоғарылығын көрсетеді. Желілік талдауда Benign (қауіпсіз трафик) класы, DoS Hulk шабуылы, DDoS шабуылы, DoS GoldenEye шабуылдары толықтай ажыратылды және модельдің тиімділігін көрсетті.

Қорытынды. Мақалада желілік шабуылдарды анықтау және оларды жіктеу мәселесі зерттелді. Осы мақсатта ЖИ негізделген бірнеше МО және DL алгоритмдері – Random Forest, SVM және CNN қолданылып, олардың тиімділігі салыстырмалы түрде талданды.

Зерттеу нәтижелері келесі негізгі **қорытындыларды** көрсетті:

- Деректерді алды ала өңдеу кезінде маңызды белгілерді іріктеу модельдердің жалпы өнімділігіне айтарлықтай әсер ететіні анықталды. Масштабтау және деректерді сандық форматқа келтіру сияқты процедуралар, әсіресе SVM және NN модельдерінің жұмысында маңызды рөл атқарды;

- SVM алгоритмі кейбір шабуыл түрлерін анықтауда жоғары нәтижелер көрсеткенімен, деректер көлемі ұлғайған сайын оның есептеу жылдамдығының төмендейтіні байқалды. Бұл фактор оны нақты уақыт режимінде жұмыс жасайтын жүйелерде қолдануды белгілі бір деңгейде шектейді;

- CNN моделі шабуылдардың күрделі құрылымдық ерекшеліктерін тиімді меңгеріп, жақсы нәтижелер көрсетті. Дегенмен, мұндай модельдерді оқыту үшін жоғары есептеу ресурстары мен қосымша уақыт керек.

Зерттеу нәтижелері көрсеткендей, желілік шабуылдарды анықтау барысында бір ғана алгоритмді қолдану жеткіліксіз болуы мүмкін. Себебі шабуылдардың сипаты, деректердің көлемі мен құрылымы өзгерген жағдайда әртүрлі модельдер әртүрлі тиімділік көрсетеді. Сондықтан болашақта нақты міндеттерге байланысты бірнеше модельді біріктіру немесе ансамбльдік тәсілдерді қолдану арқылы жүйенің сенімділігін арттыру мүмкіндігі бар.

ЖИ-ке енгізделген шешімдерді желілік қауіпсіздік саласына енгізу цифрлық инфрақұрылымды қорғаудың маңызды бағыттарының бірі болып табылады. Мұндай тәсілдер желілік аномалияларды ерте кезеңде автоматты түрде анықтауға және кибершабуылдардың алдын алуға мүмкіндік береді.

Осы бағыттағы зерттеулер болашақ интеллектуальды қауіпсіздік жүйелерінің қалыптасуына негіз болады және қосымша ғылыми зерттеулер жүргізуді талап етеді.

Сонымен қатар, зерттеу барысында ЖИ-ке негізделген МО және DL алгоритмдерінің мүмкіндіктері қарастырылды. Атап айтқанда, Random Forest, SVM сияқты дәстүрлі әдістермен қатар, NN-дің заманауи архитектурасының бірі – CNN қолданылды. Бұл алгортимдер шабуыл түрлерін жіктеу, қалыпты және аномальды желілік трафикті ажырату, сондай-ақ жаңа немесе сирек кездесетін шабуылдарды анықтау мүмкіндіктері тұрғысынан салыстармалы түрде талданды.

References

Al-Jaberi A.J.K., Kurnaz S., Naser R.A.S., et al. (2025) A novel architecture based on weight freezing and random forest for website phishing detection. *International Journal of Computational Intelligence Systems*, 18. — 284 p. https://doi.org/10.1007/s44196-025-00975-5 (in Eng.)

Aljabri M., Aljamee S.S., Mohammad R.M.A., Almotiri S.H., Mirza S., Anis F.M., Aboulnour M., Alomari D.M., Alhamed D.H., & Altamimi H.S. (2021) Intelligent techniques for detecting network attacks: Review and research directions. *Sensors*, 21. — 7070 p. https://doi.org/10.3390/s21217070 (in Eng.)

Altwaijry N., Al-Turaiki I., Alotaibi R., & Alakeel F. (2024) Advancing phishing email detection: A comparative study of deep learning models. *Sensors*, 24. — 2077 p. https://doi.org/10.3390/s24072077 (in Eng.)

Asambaev A.Zh. (2011) *Zhasandy intellekt negizderi: Okulyk* [Fundamentals of artificial intelligence: Textbook]. Almaty: Dauir. (in Kaz.)

Bolatbek M., Saginai M., & Musiralieva Sh. (2024) Using machine learning methods to detect destructive web content in the Kazakh language. *Academic Scientific Journal of Computer Science*, (4). — P. 99–111. https://doi.org/10.32014/2024.2518-1726.310 (in Eng.)

Cárdenas-Haro J.A., Salem M., Aldaco-Gastélum A.N., López-Avitia R., & Dawson M. (2024) Enhancing security in social networks through machine learning: Detecting and mitigating Sybil attacks with SybilSocNet. *Algorithms*, 17. — 442 p. https://doi.org/10.3390/a17100442 (in Eng.)

Cyber Shield (2025) Access: https://www.gov.kz/memleket/entities/knb/activities/250?lang=kk (in Eng.)

Darktrace (2025) *AI and cybersecurity: Predictions for 2025*. https://www.darktrace.com/blog/ai-and-cybersecurity-predictions-for-2025 (in Eng.)

IBM Security (2022) *Cost of a data breach report*. https://www.ibm.com/security/data-breach (in Eng.)

Issa M.M., Aljanabi M., & Muhialdeen H.M. (2024) Systematic literature review on intrusion detection systems: Research trends, algorithms, methods, datasets, and limitations. *Journal of Intelligent Systems*, 33(1). — 20230248 p. https://doi.org/10.1515/jisys-2023-0248 (in Eng.)

Kaspersky (2024) *Kaspersky predicts AI and privacy to shape consumer cybersecurity landscape in 2025*. https://www.kaspersky.com/about/press-releases/kaspersky-predicts-ai-and-privacy-to-shape-consumer-cybersecurity-landscape-in-2025 (in Eng.)

Khan M.A., & Usman M. (2021) A deep learning approach for intrusion detection using LSTM and GRU. *Sensors*, 21(15). — 5112 p. https://doi.org/10.3390/s21155112 (in Eng.)

Kuraś P., Bolanowski M., & Łoza M. (2026) Optimization of machine learning models for effective anomaly detection in industrial IoT systems. *Advances in Science and Technology Research Journal*, 20(1). — P. 203–221. https://doi.org/10.12913/22998624/210686 (in Eng.)

Matias Y. (2025) *Google Research 2025: Bolder breakthroughs, bigger impact*. https://research.google/blog/google-research-2025-bolder-breakthroughs-bigger-impact/ (in Eng.)

Muslam M. (2023) Privilege escalation attack detection and mitigation in cloud using machine learning. *IEEE Access*. https://doi.org/10.1109/ACCESS.2023.3273895 (in Eng.)

Muthukrishnan N., Maleki F., Ovens K., Reinhold C., Forghani B., & Forghani R. (2020) Brief history of artificial intelligence. *Neuroimaging Clinics of North America*, 30(4). — P. 393–399. https://doi.org/10.1016/j.nic.2020.07.004 (in Eng.)

Salem O., Alsubhi K., Shaafi A., Gheryani M., Mehaoua A., & Boutaba R. (2022) Man-in-the-middle attack mitigation in Internet of Medical Things. *IEEE Transactions on Industrial Informatics*, 18(3). — P. 2053–2062. https://doi.org/10.1109/TII.2021.3089462 (in Eng.)

Singh A., & Gupta B.B. (2022) Distributed denial-of-service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms: Issues, challenges, and future research directions. *International Journal on Semantic Web and Information Systems*, 18(1). — P. 1–43. https://doi.org/10.4018/IJSWIS.297143 (in Eng.)

Tadhani J.R., Vekariya V., Sorathiya V., et al. (2024) Securing web applications against XSS and SQLi attacks using a novel deep learning approach. *Scientific Reports*, 14. — 1803 p. https://doi.org/10.1038/s41598-023-48845-4 (in Eng.)

Ye X., Luo F., Cui H., et al. (2025) Research on insider threat detection based on personalized federated learning and behavior log analysis. *Scientific Reports*, 15. — 19214 p. https://doi.org/10.1038/s41598-025-04029-w (in Eng.)

Zhou Y. (2025) Design and implementation of computer network security monitoring system. *Journal of Computer, Signal, and System Research*, 2(4). — P. 63–68. https://doi.org/10.71222/qkantx75 (in Eng.)

Zhunisov N.M., Aben A.B., & Isakov D. (2024) Detection of network attacks using a comparative analysis of machine learning algorithms. *Mechanics and Technologies*, 4(86). — P. 430–439. https://doi.org/10.55956/ZCJD4515 (in Eng.)

Publication Ethics and Publication Malpractice
in the journals of the Central Asian Academic Research Center LLP

For information on Ethics in publishing and Ethical guidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the journals of the Central Asian Academic Research Center LLP implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The Central Asian Academic Research Center LLP follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the Central Asian Academic Research Center LLP.

The Editorial Board of the Central Asian Academic Research Center LLP will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:
www:nauka-nanrk.kz
http://physics-mathematics.kz/index.php/en/archive
ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Ответственный редактор *А. Ботанқызы*
Редакторы: *Д.С. Аленов, Т. Апендиев*
Верстка на компьютере: *Г.Д. Жадырановой*

Подписано в печать 31.03.2026.
Формат 60x881/8.
20,0 п.л. Заказ 1.

«Central Asian Academic Research Center» LLP
Алматы, Шевченко к-сі, 28