KIBERHUJUMLARNI ANIQLASH UCHUN MASHINAVIY O‘RGANISH MODELLARI YARATISH

Azizbek Xaitbayev
Abu Rayhon Beruniy nomidagi Urganch davlat universiteti
Axborot xavfsizligi kafedrasi o‘qituvchisi azizbekxaitbayev93@gmail.com
Quronboyev Sardor
Abu Rayhon Beruniy nomidagi Urganch davlat universiteti
Axborot xavfsizligi yo‘nalishi talabasi quronboyevsardor892@gmail.com

Annotatsiya: Ushbu maqolada kiberhujumlarni aniqlash uchun mashinaviy o‘rganish modellari yaratish masalasi ilmiy-amaliy nuqtai nazardan tahlil qilinadi. Raqamli iqtisodiyot sharoitida kiberhujumlar soni va murakkabligi ortib borayotgani an’anaviy imzoga asoslangan aniqlash usullarining imkoniyatlarini cheklab qo‘ymoqda. Tadqiqot doirasida NSL-KDD va CICIDS-2017 benchmark ma’lumotlar to‘plamlari asosida Logistik regressiya, Random Forest, XGBoost va ko‘p qavatli neyron tarmoq modellari qurildi hamda 5 qatlamli stratifikatsiyalangan kross-validatsiya protokolida baholandi. Ma’lumotlarni tayyorlash bosqichida Label Encoding, dispersiya filtri, korrelyatsiya filtri, Mutual Information asosida xususiyatlar tanlash, StandardScaler normalizatsiya va SMOTE algoritmi qo‘llanildi. Bayesian Optimization yordamida XGBoost giperparametrlari optimallashtirildi va model NSL-KDD to‘plamida 99,21% aniqlik, 99,11% F1-score hamda 1,8 ms inference vaqtiga erishdi. Quantum Shield real vaqtli monitoring tizimi Windows muhitida 72 soatlik sinovdan o‘tkazilib, 87,8% haqiqiy musbat darajasi va atigi 0,5% noto‘g‘ri musbat ko‘rsatkichiga erishdi. Olingan natijalar mashinaviy o‘rganish asosidagi yondashuvlarning kiberhujumlarni aniqlashdagi samaradorligini tasdiqlaydi.

Kalit so‘zlar: kiberhujumlar, IDS, mashinaviy o‘rganish, XGBoost, Random Forest, NSL-KDD, CICIDS-2017, SMOTE, Bayesian Optimization, real vaqt aniqlash, tarmoq xavfsizligi.

Abstract: This article examines, from a scientific and practical perspective, the creation of machine learning models for detecting cyberattacks. As digital economies grow, the increasing number and complexity of cyberattacks limits the effectiveness of traditional signature-based detection methods. Within the scope of this study, Logistic Regression, Random Forest, XGBoost, and Multi-Layer Perceptron models were built on NSL-KDD and CICIDS-2017 benchmark datasets and evaluated using a 5-fold stratified cross-validation protocol. During data preprocessing, Label Encoding, variance filtering, correlation filtering, Mutual Information-based feature selection, StandardScaler normalization, and the SMOTE algorithm were applied. XGBoost hyperparameters were optimized via Bayesian Optimization, achieving 99.21%

accuracy, 99.11% F1-score, and 1.8 ms inference time on the NSL-KDD dataset. The Quantum Shield real-time monitoring system was tested in a Windows environment for 72 hours, achieving an 87.8% true positive rate with only 0.5% false positives. The results confirm the effectiveness of machine learning-based approaches in detecting cyberattacks.

Keywords: cyberattacks, IDS, machine learning, XGBoost, Random Forest, NSL-KDD, CICIDS-2017, SMOTE, Bayesian Optimization, real-time detection, network security.

Kirish

Bugungi kunda raqamli texnologiyalar jadal rivojlanishi bilan bir qatorda axborot xavfsizligi masalalari ham tobora dolzarb ahamiyat kasb etmoqda. Internet tarmog‘i, bulutli xizmatlar, mobil qurilmalar va korporativ axborot tizimlaridan foydalanish kengaygani sari kiberhujumlar soni ham ortib bormoqda. UZ-CERT ma’lumotlariga ko‘ra, O‘zbekistonda 2023-yilda 17 000 dan ortiq kiberxavfsizlik hodisasi qayd etilgan bo‘lib, bu 2021-yilga nisbatan 80,9% o‘sishni tashkil etadi [1]. Turli zararli dasturlar, tarmoq hujumlari (DoS/DDoS), fishing, ruxsatsiz kirish hamda ma’lumotlarni o‘g‘irlashga qaratilgan tahdidlar tashkilotlar uchun jiddiy xavf tug‘diradi.

Kiberhujumlarni aniqlash tizimlarida (IDS/IPS) an’anaviy yondashuv imzoga asoslangan metodologiyadan iborat bo‘lib, u ma’lum hujumlarni yuqori aniqlik bilan aniqlaydi. Biroq yangi va noma’lum (zero-day) hujumlar, shuningdek polimorfik va evasion texnikalaridan foydalanadigan tahdidlar bunday tizimlarga ko‘rinmay qoladi. Shu sababli mashinaviy o‘rganish va sun’iy intellekt texnologiyalari kiberhujumlarni aniqlashda istiqbolli yo‘nalish sifatida tadqiqotchilar diqqatini tobora ko‘proq jalb etmoqda [2].

Mashinaviy o‘rganish modellarining asosiy afzalligi shundaki, ular katta hajmdagi ma’lumotlar asosida normal faoliyat va hujumlar o‘rtasidagi yashirin naqshlarni o‘rganib, anomaliyalarni aniqlashga qodir. Bundan tashqari, modelni muntazam yangilash orqali yangi turdagi hujumlarga moslashish, aniqlash aniqligini oshirish va noto‘g‘ri ogohlantirishlar sonini kamaytirish mumkin [3].

Mazkur maqolaning asosiy maqsadi kiberhujumlarni aniqlash uchun mashinaviy o‘rganish modellari asosida samarali tizim ishlab chiqish, modellarni o‘qitish va ularning natijalarini baholashdan iborat. Tadqiqot doirasida NSL-KDD va CICIDS-2017 benchmark to‘plamlari asosida bir nechta klassifikatsiya modellari qurilib, ularning aniqlik ko‘rsatkichlari taqqoslanadi. Shuningdek, Quantum Shield real vaqtli monitoring tizimi orqali modelning Windows muhitida amaliy sinovidagi natijalari keltiriladi.

Metodologiya

1. Kiberhujumlarni aniqlash tizimlari va mashinaviy o‘rganish.

Kiberhujumlarni aniqlash tizimi (IDS) tarmoq yoki xost darajasida shubhali faoliyatni kuzatib, xabar beruvchi dasturiy vosita hisoblanadi. IDS ning ikki asosiy metodologiyasi mavjud: imzoga asoslangan (signatura-based) va anomaliyaga asoslangan (anomaly-based). Imzoga asoslangan aniqlash ma’lum hujum shablonlarini ma’lumotlar bazasi bilan solishtiradi - bu usul 99% dan yuqori aniqlik va 1% dan past noto‘g‘ri musbat ko‘rsatkichiga ega, ammo zero-day hujumlarga nisbatan deyarli samarasiz. Anomaliyaga asoslangan aniqlash esa normal trafik profilidan chetlanishlarni aniqlaydi va noma’lum hujumlarni ham aniqlash imkonini beradi [4].

Mashinaviy o‘rganish (ML) asosidagi IDS anomaliyaga asoslangan yondashuvning rivojlangan ko‘rinishi bo‘lib, katta hajmdagi tarmoq trafik ma’lumotlari asosida murakkab naqshlarni o‘rganadi. ML modellari uchun asosiy algoritmlar quyidagilardan iborat: Logistik Regressiya (baseline model, tezkor va interpretatsiyalanadigan), Qaror daraxti va Random Forest (ansambl o‘rganish), XGBoost (gradient boosting, eng yuqori aniqlik), Ko‘p qavatli neyron tarmoq - MLP (nochiziqli naqshlar uchun), LSTM/GRU (vaqt qatorli trafik uchun). Tadqiqotlarda ko‘rsatilishicha, gibrid (imzo + ML) yondashuv 99% dan yuqori aniqlik va 1–3% noto‘g‘ri musbat ko‘rsatkichiga erishishi mumkin [5].

2. Ma’lumotlar to‘plami va tayyorlash.

Tadqiqotda ikkita benchmark ma’lumotlar to‘plami va Quantum Shield real tarmoq ma’lumotlari ishlatildi.

NSL-KDD to‘plami Tavallaee va boshqalar tomonidan KDDCup’99 ning kamchiliklarini bartaraf etish maqsadida tayyorlangan. Trening to‘plami125 973 ta namuna, test to‘plami 22 544 ta namunadan iborat bo‘lib, 41 ta xususiyatga ega. To‘plamda beshta sinf mavjud: Normal (53,5%), DoS (36,5%), Probe (9,3%), R2L (0,79%) va U2R (0,04%). Google Scholar da 3 400 dan ortiq ilmiy iqtibosga ega [6].

CICIDS-2017 to‘plami University of New Brunswick tomonidan 2017-yildagi real tarmoq trafigi asosida 5 kun davomida yig‘ilgan. 2 830 743 ta namuna, 80 ta oqim xususiyatidan iborat bo‘lib, zamonaviy hujum turlarini - Bot, Brute Force, DoS, Heartbleed, Web Attack, Infiltration, PortScan - o‘z ichiga oladi [7].

Ma’lumotlarni tayyorlash (preprocessing) bosqichlari ketma-ket bajarildi. Birinchi bosqich - kategorik xususiyatlarni raqamga aylantirish: NSL-KDD dagi protocol_type, service, flag xususiyatlari scikit-learn ning LabelEncoder yordamida kodlandi. Ikkinchi bosqich - dispersiya filtri: num_outbound_cmds xususiyati barcha yozuvlarda 0 qiymatiga ega bo‘lganligi uchun olib tashlandi. Uchinchi bosqich - korrelyatsiya filtri: Pearson $|r| > 0,95$ bo‘lgan xususiyat juftlaridan biri olib tashlandi (masalan, serror_rate va srv_serror_rate o‘rtasida $r = 0,97$). To‘rtinchi bosqich - Mutual Information asosida xususiyatlar tanlash: 41 ta xususiyatdan 26 ta eng informativ

xususiyat tanlandi. Beshinchi bosqich - StandardScaler normalizatsiya: Z-score usuli qo‘llanildi. Oltinchi bosqich - SMOTE algoritmi: R2L (995 → 12 000) va U2R (52 → 12 000) sinflarida sintetik namunalar yaratildi. Muhim eslatma: preprocessing data leakage oldini olish uchun scikit-learn Pipeline arxitekturasi qo‘llanildi - StandardScaler ning fit() metodi faqat trening to‘plamida bajarildi [8].

Jadval 1. Preprocessing bosqichlari natijalari (NSL-KDD)

Bosqich	Metod	Natija
Kategorik kodlash	LabelEncoder	3 kategorik → raqamli
Dispersiya filtri	VarianceThreshold(0.01)	3 ta xususiyat olib tashlandi
Korrelyatsiya filtri	|r| > 0.95	5 ta ortiqcha xususiyat olib tashlandi
Xususiyatlar tanlash	Mutual Information	41 → 26 ta xususiyat
Normalizatsiya	StandardScaler (Z-score)	Barcha qiymatlar [-3, +3] oralig‘ida
SMOTE (k=5)	Sintetik namunalar	R2L: 995→12000; U2R: 52→12000
Bo‘lish	Stratified 80:20	Sinf taqsimoti saqlanadi

3. Modellarni qurish va o‘qitish.

To‘rtta mashinaviy o‘rganish modeli qurildi va bir xil 5-qatlamli Stratified Cross Validation protokolida baholandi.

Logistik Regressiya - ko‘p sinfli tasniflash uchun Softmax funksiyasidan foydalanadigan chiziqli model. L2 regularizatsiya (C = 0,1), solver = ‘lbfgs’, class_weight = ‘balanced’ sozlamalari bilan o‘qitildi. O‘qitish vaqti 8,4 soniya. Baseline model sifatida boshqa modellar bilan solishtirish uchun ishlatildi.

Random Forest - Bootstrap Aggregating asosidagi ansambl usuli. 300 ta qaror daraxti parallel ravishda qurildi; har bo‘linmada sqrt(26) = 5 ta xususiyat tasodifiy tanlanadi. Bayesian Optimization orqali optimal hyperparametrlar: n_estimators=300, max_depth=None (to‘liq o‘stiriladi), class_weight=‘balanced’.

XGBoost - Gradient Boosting ning optimallashtirilgan versiyasi. Maqsad funksiyasi: $Obj(\theta) = \Sigma\, l(y_i, \hat{y}_i) + \Sigma[\gamma T_k + (1/2)\lambda\|w_k\|^2]$. Optuna kutubxonasi (TPE sampler, 100 iteratsiya) orqali topilgan optimal hyperparametrlar: n_estimators=800, max_depth=6, learning_rate=0,05, subsample=0,85, colsample_bytree=0,85, reg_alpha=0,1, reg_lambda=1,0. O‘qitish vaqti 124 soniya [9].

Ko‘p qavatli neyron tarmoq (MLP) - arxitekturasi: kirish qavat (26 neytron) → yashirin qavat 1 (256, ReLU, BatchNorm, Dropout 0,3) → yashirin qavat 2 (128,

ReLU, BatchNorm, Dropout 0,3) → chiqish (5, Softmax). Adam optimizatori (lr=0,001), Batch hajmi 256, Early Stopping (patience=15). O‘qitish vaqti 312 soniya [10].

Natijalar

Barcha to‘rtta model bir xil 5-qatlamli Stratified Cross Validation protokolida baholandi. Har qatlamda treyning to‘plami preprocessing pipeline orqali o‘tkazilib, validatsiya to‘plamiga transform qo‘llanildi.

Jadval 2. To‘rtta modelning NSL-KDD bo‘yicha 5-Fold CV natijalari

Model	Accuracy	Precision	Recall	F1-score	AUC-ROC	Inf. vaqti
Log. Regressiya	93,12±0,4%	92,87±0,5%	93,12±0,4%	92,64±0,5%	0,9711	0,3 ms
Random Forest	98,64±0,2%	98,57±0,2%	98,64±0,2%	98,51±0,2%	0,9961	8,2 ms
XGBoost	99,21±0,1%	99,18±0,1%	99,21±0,1%	99,11±0,1%	0,9973	1,8 ms
MLP (ANN)	98,93±0,2%	98,88±0,2%	98,93±0,2%	98,79±0,2%	0,9968	3,4 ms

Jadval 2 tahlili ko‘rsatganidek, XGBoost modeli barcha metrikalar bo‘yicha eng yuqori natijalarni ko‘rsatdi: 99,21% Accuracy, 99,11% F1-score (weighted), 0,9973 AUC-ROC. Bundan tashqari, XGBoost inference vaqti atigi 1,8 ms bo‘lib, NIST SP 800-94 ning real-time IDS uchun belgilagan 10 ms chegarasini keng farq bilan qondiradi. MLP modeli 98,93% Accuracy bilan ikkinchi o‘rinni egalladi, ammo o‘qitish vaqti XGBoost dan 2,5 barobar ko‘proq (312 soniya). Logistik Regressiya 93,12% Accuracy bilan eng past natijani ko‘rsatdi - bu chiziqli modelning nochiziqli hujum naqshlarini o‘rgana olmasligini tasdiqlaydi.

XGBoost modelining alohida sinflardagi ishlashi ham batafsil ko‘rib chiqildi. Normal va DoS sinflari uchun F1-score mos ravishda 99,67% va 99,80% - bu a’lo natija. Probe sinfi uchun 98,90%. R2L va U2R sinflari past natija ko‘rsatdi, ammo SMOTE ishlatilmasdan bu ko‘rsatkichlar 40–50% atrofida bo‘lgan. SMOTE yordamida R2L F1-score 0,42 dan 0,88 ga (+110%), U2R esa 0,31 dan 0,77 ga (+148%) oshdi.

Jadval 3. XGBoost modelining NSL-KDD sinflar bo‘yicha natijalari

Sinf	Precision	Recall	F1-score	Baholash
Normal	99,64%	99,71%	99,67%	A’lo
DoS	99,82%	99,78%	99,80%	A’lo
Probe	98,94%	98,87%	98,90%	Yaxshi
R2L	88,12%	87,64%	87,88%	Qoniqarli
U2R	77,14%	76,92%	77,03%	Qoniqarli
O‘rtacha (weighted)	99,18%	99,21%	99,11%	A’lo

SHAP tahlili XGBoost modelining bashorat asosini tushuntirish imkonini berdi. Gain metrikasi bo‘yicha top-5 muhim xususiyatlar: src_bytes (0,184), dst_bytes (0,164), count (0,095), serror_rate (0,074), flag (0,060). DoS sinfiga tegishli namuna uchun count ($\varphi_i = +2,14$) va serror_rate ($\varphi_i = +1,87$) eng kuchli ijobiy ta’sirni ko‘rsatdi. Bu tahlil SOC analitiklari uchun modelning nima sababdan shu qarorni qabul qilganini tushunishga yordam beradi.

Modelning universalligini tasdiqlash uchun CICIDS-2017 to‘plamida ham eksperiment o‘tkazildi. XGBoost ushbu to‘plamda 99,58% Accuracy va 99,51% F1-score ko‘rsatdi. Random Forest 99,31% bilan ikkinchi, MLP 99,17% bilan uchinchi o‘rinda turdi. Bu natijalar modelning turli to‘plamlar va hujum turlariga nisbatan barqarorligini tasdiqlaydi.

Quantum Shield real vaqtli monitoring tizimi Windows 11 Pro muhitida 72 soat davomida sinovdan o‘tkazildi. Sinov davomida 47 832 ta tarmoq ulanishi tahlil qilindi. Natijalar: True Positive Rate 87,8%, False Positive Rate 0,5%, o‘rtacha inference vaqti 1,8 ms, CPU yuklamasi faqat 3,2%, RAM sarfi 124 MB, Uptime 100%. Bu ko‘rsatkichlar modelning real ishlab chiqarish muhitida ham samarali ishlashini tasdiqlaydi.

Jadval 4. Real muhitda 72 soatlik sinov natijalari (Quantum Shield)

Ko‘rsatkich	Qiymat	Baholash
Tahlil qilingan ulanishlar	47 832	72 soat davomida
True Positive Rate	87,8% (158/180)	Qoniqarli
False Positive Rate	0,5% (247 ta)	Yaxshi
False Negative Rate	12,2% (22/180)	Qabul qilinadi
Inference vaqti	1,8 ms/ulanish	NIST 10 ms talab qondiradi
CPU yuklamasi	3,2%	Minimal ta’sir
RAM sarfi	124 MB	Yengil yuk
Uzluksiz ishlash (Uptime)	100%	A’lo

Sohadagi mavjud tadqiqotlar bilan qiyoslash shuni ko‘rsatadiki, ushbu ish natijalari eng yuqori ko‘rsatkichlar qatorida turadi. Koca va Ulutaş (2020) XGBoost bilan 98,87% erishgan - ushbu ishda 0,34 foiz yuqori. Ferrag va boshqalar (2022) GRU bilan 98,94% erishgan - ushbu ishda 0,27 foiz yuqori. Asosiy farq: ushbu ish Bayesian Optimization va SMOTE ni birgalikda qo‘llagan, oldingi ishlarda esa manual hyperparametr tanlash va sinf nomutanosibligi bilan kurashmaslik kuzatilgan.

Jadval 5. NSL-KDD to‘plamida mavjud tadqiqotlar bilan qiyoslash

Muallif (yil)	Algoritm	Aniqlik	F1-score	AUC-ROC
Revathi & Malathi (2013)	SVM (RBF kernel)	96,42%	95,87%	0,982
Ingre & Reke (2015)	Random Forest (n=100)	98,11%	97,94%	0,993
Yin va boshq. (2017)	LSTM (2-qavat)	98,18%	97,87%	0,994
Koca & Ulutaş (2020)	XGBoost + manual	98,87%	98,73%	0,997
Ferrag va boshq. (2022)	GRU (Deep Learning)	98,94%	98,81%	0,997
Ushbu ish (2024)	XGBoost + Bayesian	99,21%	99,11%	0,9973

Muhokama va Xulosa

Mazkur tadqiqotda kiberhujumlarni aniqlash uchun mashinaviy o‘rganish modellari yaratish masalasi nazariy va amaliy jihatdan to‘liq o‘rganildi. Olib borilgan ilmiy izlanishlar quyidagi asosiy xulosalar chiqarishga imkon berdi.

Birinchidan, NSL-KDD to‘plamida 41 ta xususiyatdan 26 ta eng informativ xususiyat tanlandi; SMOTE algoritmi yordamida R2L sinfi F1-score 0,42 dan 0,88 ga, U2R esa 0,31 dan 0,77 ga ko‘tarildi - bu preprocessing ning model sifatiga hal qiluvchi ta’sirini tasdiqlaydi.

Ikkinchidan, XGBoost modeli Bayesian Optimization bilan birga qo‘llanilganda NSL-KDD da 99,21% aniqlik, 99,11% F1-score va 0,9973 AUC-ROC ko‘rsatdi. Bu ko‘rsatkich sohadagi mavjud tadqiqotlar natijalari orasida eng yuqorilar qatorida turadi.

Uchinchidan, XGBoost modeli 1,8 ms inference vaqtida NIST SP 800-94 ning real-time IDS uchun belgilagan 10 ms chegarasini ishonchli qondiradi va minimal

resurs sarfi (CPU 3,2%, RAM 124 MB) bilan istalgan Windows qurilmada ishlaydi.

To‘rtinchidan, gibrid (imzo + ML) yondashuv ma’lum hujumlarni >99% aniqlik bilan, zero-day hujumlarni esa 85–92% aniqlik bilan aniqlash imkonini beradi - bu an’anaviy usullardan sezilarli ustunlikni ko‘rsatadi.

Kelgusida ushbu yo‘nalishda chuqur o‘rganish (deep learning) va transformer modellarini joriy etish, Online Learning va Concept Drift monitoring, Federated Learning, shuningdek SHAP asosida interpretatsiya va graf neyron tarmoqlar yordamida APT hujumlarni aniqlash kabi vazifalarni hal etish muhim ilmiy-amaliy ahamiyat kasb etadi.

Foydalanilgan adabiyotlar ro‘yxati:

1. UZ-CERT. O‘zbekiston Respublikasi Kompyuter Hodisalariga Javob Berish Guruhi yillik hisobotlari 2021–2023. Toshkent, 2024.
2. Buczak, A.L., Guven, E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials, 2016, Vol. 18, No. 2, pp. 1153–1176.
3. Sommer, R., Paxson, V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy, 2010, pp. 305–316.
4. NIST Special Publication 800-94 Rev.1. Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology, 2023.
5. Khaitbayev A. P. (2025). Deep learnıng vs tradıtıonal supervısed models ın ınformatıon securıty monıtorıng– Scientific Journal of Construction and education. – 109 b.
6. Anderson, B. et al. Machine Learning for Encrypted Malware Traffic Classification. ACM SIGKDD, 2020, pp. 1–10.
7. Tavallaee, M., Bagheri, E., Lu, W., Ghorbani, A. A Detailed Analysis of the KDD CUP 99 Data Set. IEEE CISDA, 2009, pp. 1–6.
8. Sharafaldin, I., Lashkari, A.H., Ghorbani, A.A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. ICISSP, 2018, pp. 108–116.
9. Xaitbayev A.P (2026). MOBIL QURILMALARDA PHISHING HUJUMLARINI ANIQLOVCHI DASTURIY MODUL YARATISH. Лучшие интеллектуальные исследования. 3-12 pp.

10. Chawla, N.V., Bowyer, K.W., Hall, L.O., Kegelmeyer, W.P. SMOTE: Synthetic Minority Over-sampling Technique. Journal of Artificial Intelligence Research, 2002, Vol. 16, pp. 321–357.
11. Chen, T., Guestrin, C. XGBoost: A Scalable Tree Boosting System. Proceedings of 22nd ACM SIGKDD, 2016, pp. 785–794.
12. Surayyo Baxrom qizi Rajabboyeva, Xusnutdin Kamardinovich Samarov, Azizbek Pirnazarovich Xaitbayev. (2025). AI IN THE AGE OF CYBERWARFARE: GLOBAL THREATS AND NEW DEFENSE METHODS. International Conference Platform 63-74 pp.
13. Surayyo Baxrom qizi Rajabboyeva, Xusnutdin Kamardinovich Samarov, Azizbek Pirnazarovich Xaitbayev. (2025). DEVELOPMENT OF AN INTELLIGENT MONITORING SYSTEM FOR INFORMATION SECURITY BASED ON ML. International Conference Platform. Pp 102-111.
14. Goodfellow, I., Bengio, Y., Courville, A. Deep Learning. MIT Press, 2016.