ISNN 3030-3907

2026/4
VOLUME 4

DEVELOPMENT OF SCIENCE

ILMIY JURNAL



Development of science

Ilmiy jurnal

2026/4 VOLUME 4

ISSN 3030 -3907

Ilmiy jurnal OAK rayosatining 2024 yil 27 sentabrdagi 361-son qaroriga asosan 02.00.00 kimyo fanlari hamda 2025 yil 12 fevral 367- son qaroriga asosan 05.00.00 texnika fanlari bo‘yicha falsafa doktori (PhD) va fan doktori (DSc) ilmiy darajasiga talabgorlarning dissertatsiya ishlari yuzasidan dissertatsiyalari asosiy ilmiy natijalarini chop etish tavsiya etilgan milliy ilmiy nashrlar ro‘yxatiga kiritilgan.

BOSH MUHARRIR:
Temirov Alisher Hoshim o‘g‘li – texnika fanlari falsafa doktori (PhD),Dotsent.
TAHRIRIYAT KENGASH RAISI:
Fozilov Sadriddin Fayzullayevich – texnika fanlari doktori, professor
TAHRIRIYAT KENGASH A’ZOLARI

TEXNIKA FANLARI/ TECHNICAL SCIENCES/ ТЕХНИЧЕСКИЕ НАУКИ

Bozorov G‘ayrat Rashidovich
Buxoro Davlat Texnika Universiteti, professor
Abdurahmonov Olim Rustamovich
Buxoro Davlat Texnika Universiteti, professor
Adizov Bobur Zamirovich
O‘zbekiston Respublikasi Fanlar akademiyasi Umumiy va noorganik kimyo instituti, professor
Hayitov Ruslan Rustamjonovich
Buxoro Davlat Texnika Universiteti, professor
Jumayev Qayum Karimovich
Buxoro Davlat Texnika Universiteti, professor.
Berdiyev Dorob Murodovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor
Maxmudov Rafiq Amonovich
Buxoro Davlat Texnika Universiteti, professor.
Tilloyev Lochin Ismatilloyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Raxmonov Qahramon Sanakulovich
Buxoro Davlat Texnika Universiteti, dotsent.
Barakayev Nusratullo Rajabovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor.
Jo‘rayev Xayrullo Fayziyevich
Buxoro Davlat Texnika Universiteti, professor.
Panoyev Erali Rajabboyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Ataullayev Sherzod Nabiullyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Malik Negmurodovich
Buxoro Davlat Texnika Universiteti, dotsent.
Axmedova Ozoda Bahronovna
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti.
Safarov Bahri Jumayevich
Buxoro Davlat Texnika Universiteti, dotsent.
Xaydarov Axtam Amonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Safarov Jasur Alijon o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Асадова Раъно Дилмуратовна
Тошкент Давлат техника университети доценти

KIMYO FANLARI/ CHEMICAL SCIENCES/ ХИМИЧЕСКИЕ НАУКИ

Axmedov Voxid Nizomovich
Buxoro Davlat Texnika Universiteti, professor
Umarov Baqo Bafoyevich
Buxoro Davlat Universiteti, professor
Kodirov Abduaxad Abduraximovich
Qarshi davlat Universiteti, professor
Qurbonov Mingniqul Jumagulovich
Qarshi davlat Universiteti, dotsent
Turemuratov Sharibay Naurizbaevich
O‘zbekiston Respublikasi Fanlar akademiyasi Qoraqalpog‘iston bo‘limi Bosh ilmiy kotibi, professor
Tursunov Kaxor Shonazarovich
Qarshi davlat Universiteti, professor
Do‘stov Hamro
Buxoro Davlat Texnika Universiteti, professor
Panoyev Nodir Shavkatovich
Buxoro Davlat Texnika Universiteti, dotsent.
Olimov Bobur Bahodir o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Kasimov Sherzod Abduazimovich
Termiz Davlat Universiteti, professor.
Aliqulov Rustam Valiyevich
Termiz Davlat Universiteti, professor
Tropov Xamza Tursunovich
Samarqand Davlat Universiteti, professor

IQTISODIYOT FANLARI/ ECONOMICS/ ЭКОНОМИЧЕСКИЕ НАУКИ

Nizamov Aslitdin Badreddinovich
Buxoro Davlat Texnika Universiteti, professor.
Boboyev Akmal Choriyevich
Buxoro Davlat Texnika Universiteti, professor.
Ergashxojayeva Shaxnoza Djasurovna
Toshkent davlat iqtisodiyot universiteti, professor
Saidaxmedova Nodira Ilxomovna
Toshkent davlat iqtisodiyot universiteti, professor
Muxsinov Bekzod Toxirovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shakarov Qulmat Ashirovich
Renessans ta'lim universiteti,dotsent.
Jumaeva Zulfiya Qayumovna
Buxoro Davlat Texnika Universiteti, dotsent.
Norova Salomat Yusupovna
Buxoro Davlat Texnika Universiteti, dotsent.
Avezova Shaxnoza Maxmudjonovna
Buxoro Davlat Texnika Universiteti, dotsent.
Jalilov Jamshid G‘anijonovich
Toshkent davlat iqtisodiyot universiteti, dotsent
Xasanova Gulruh Djumanazarovna
Buxoro Davlat Texnika Universiteti, dotsent.

PEDAGOGIKA FANLARI/ PEDAGOGICAL SCIENCES / ПЕДАГОГИЧЕСКИЕ НАУКИ

Siddiqova Sadoqat G‘afforovna
Buxoro Davlat Texnika Universiteti, dotsent.
Zoyirov Erkin Xalilovich
Buxoro Davlat Texnika Universiteti, DSc, professor
Gaffarov Feruz Hasanovich
Puchon Universiteti, *professor*
Ruziyev Davron Yuldashevich
Buxoro Davlat Universiteti, professor
Muradova Firuza Rashidovna
Buxoro Davlat Texnika Universiteti, professor.
Yunusova Gulandon Samiyevna
Buxoro Davlat Texnika Universiteti, professor.
To‘xtayeva Zebo Sharifovna
Buxoro Davlat Texnika Universiteti, professor.
Navro‘zova Gulchixra Nigmatovna
Buxoro Davlat Texnika Universiteti, dotsent.
Uzoqova Laylo Polvonovna
Buxoro muhandislik – texnologiya instituti, dotsent.
To‘raqulova Marjona Qiyom qizi
Buxoro Davlat Texnika Universiteti, dotsent.
Muradova Zarina Rashidovna
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Sanjar Aslonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shodiyev Jahongir Jo‘raqulovich
Buxoro Davlat Texnika Universiteti, dotsent
Gaffarov Laziz Hasanovich
Buxoro muhandislik – texnologiya instituti, dotsent.

Tahririyat a’zolarning to‘liq ro‘yxati jurnalning www.devos.uz saytida keltirilgan.

Tahririyat hay’ati a’zolarining tarkibini o‘zgartirish hamda qo‘shimcha kiritish yoki tahririyat a’zoligidan chiqarish bosh muharrir tomonidan amalga oshiriladi.

ISSN 3030-3907

Development of science ilmiy jurnali 2024 yil 15 aprel kuni №256445 sonli guvohnoma bilan Davlat ro‘yxatidan o‘tgan.

To‘plam elektron ko‘rinishda (pdf formatida) mualliflarga taqdim etiladi. To‘plamga kiritiladigan maqolalarning mazmuni, ulardagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligiga hamda har qanday fikr - mulohazalarga mualliflarning o‘zlari mas’ul hisoblanadilar. Talablarga javob bermaydigan maqolalar to‘plamga kiritilmaydi. Tashkiliy qo‘mita maqola matnini qisqartirish, qisman tuzatish kiritish, seksiyalarga joylashtirish huquqiga ega.

ISSN 3030-3907

TARMOQ TRAFIGIDAGI KIBERHUJUMLARNI ANIQLASHDA MASHINALI O'QITISH ALGORITMLARINI TAQQOSLASH: PAST KECHIKISH VA NOTO'G'RI TREVOGA MUAMMOLARI

Samarov Xusnutdin Kamardinovich
Muhammad al-Xorazmiy nomidagi TATU "Axborot xavfsizligi" kafedrasi dotsenti, t.f.n.
Email: samarov07@gmail.com
Surayyo Rajabboyeva Baxrom qizi
Muhammad al-Xorazmiy nomidagi TATU tayanch doktoranti
Email: surayyobaxromqizi@gmail.com
Xaitbayev Azizbek Pirnazarovich
Abu Rayhon Beruniy nomidagi Urganch davlat universiteti o'qituvchisi
Email: azizbekxaitbayev93@gmail.com

Annotatsiya. Ushbu maqolada tarmoq trafigidagi DoS, Probe, U2R va R2L kiberhujumlarini aniqlashda mashinali o'qitish algoritmlarining qiyosiy tahlili keltirilgan. Isolation Forest, Autoencoder, XGBoost, Random Forest, SVM va LSTM algoritmlari aniqlik, F1-o'lchov, kechikish vaqti va noto'g'ri trevoga darajasi bo'yicha NSL-KDD ma'lumotlar to'plami asosida baholangan. XGBoost 97–99% aniqlik va 3 ms dan past kechikish bilan eng maqbul yechim sifatida aniqlangan. Noto'g'ri trevoga darajasini kamaytirish uchun xususiyatlarni tanlash, chegaraviy qiymatni optimallashtirish, kaskadli ansambl tasniflash va SMOTE usullari tavsiya etiladi. Tadqiqot natijalari real vaqtli kiberhujumlarni aniqlash tizimlarini loyihalash uchun amaliy ko'rsatmalar beradi.

Kalit so'zlar: kiberhujumlarni aniqlash, mashinali o'qitish, intrusion detection system, Isolation Forest, XGBoost, Autoencoder, false positive, past kechikish, tarmoq xavfsizligi, NSL-KDD, SMOTE, ansambl metodlar.

Аннотация. В данной статье представлен сравнительный анализ алгоритмов машинного обучения для обнаружения кибератак типа DoS, Probe, U2R и R2L в сетевом трафике. Алгоритмы Isolation Forest, Autoencoder, XGBoost, Random Forest, SVM и LSTM оцениваются по точности, F1-мере, задержке вывода и уровню ложных срабатываний на основе набора данных NSL-KDD. Установлено, что XGBoost обеспечивает наилучший баланс показателей: точность 97–99% при задержке менее 3 мс. Для снижения ложных срабатываний предлагается комбинация методов отбора признаков, оптимизации порогового значения, каскадной ансамблевой классификации и балансировки классов с помощью SMOTE.

Ключевые слова: обнаружение кибератак, машинное обучение, система обнаружения вторжений, Isolation Forest, XGBoost, Autoencoder, ложные

ISSN 3030-3907

срабатывания, низкая задержка, сетевая безопасность, NSL-KDD, SMOTE, ансамблевые методы.

Abstract. This paper examines how well several machine learning algorithms perform when identifying network-based cyber attacks, specifically DoS, Probe, U2R, and R2L traffic. Six methods — Isolation Forest, Autoencoder, XGBoost, Random Forest, SVM, and LSTM — were tested against the NSL-KDD benchmark and assessed on detection accuracy, F1-score, inference latency, and false positive rate. Among the candidates, XGBoost showed the strongest overall results, reaching roughly 97–99% accuracy while keeping inference time under 3 ms. To bring down false alarm rates, the paper explores a combined approach: targeted feature selection, ROC-based threshold adjustment, a two-stage cascade classifier, and SMOTE oversampling for minority classes. Taken together, the findings offer some practical direction for anyone trying to build or improve a real-time intrusion detection system.

Keywords: cyber attack detection, machine learning, intrusion detection system, Isolation Forest, XGBoost, Autoencoder, false positive, low latency, network security, NSL-KDD, SMOTE, ensemble methods.

INTRODUCTION.

As network infrastructure has grown in scale and complexity over the past decade, so too has the threat landscape. Cyber attacks are more frequent, more targeted, and in many cases harder to attribute than they were even five years ago. Intrusion Detection Systems (IDS) sit at the heart of most defensive architectures, yet the signature-based approaches that dominated early IDS design have a well-known limitation: they cannot catch what they have not seen before. New attack variants, obfuscated payloads, and polymorphic malware regularly slip past rule-based filters because the underlying signatures simply do not match [1]. This has pushed researchers and practitioners toward anomaly detection grounded in machine learning, where the model learns what normal traffic looks like and raises an alert when something deviates meaningfully from that baseline.

Most comparative studies in this space rely on either NSL-KDD or UNSW-NB15 as their evaluation corpus. Both datasets organise malicious traffic into recognisable categories: DoS attacks, which flood bandwidth or processing capacity to deny service; Probe attacks, low-volume scans designed to map the network and uncover exploitable weaknesses; U2R incidents, where an attacker with a legitimate user account manages to escalate to root privileges; and R2L cases, in which an outsider gains some foothold on a local machine by exploiting a remote service vulnerability [2]. Each of these categories leaves a different

ISSN 3030-3907

fingerprint in traffic data, and no single algorithm handles all four equally well — which is one of the things this study tries to make clearer.

A gap that appears repeatedly in the literature is the absence of latency data alongside accuracy figures. Knowing that a classifier reaches 97% macro-accuracy is useful; knowing whether it can do so in under five milliseconds per sample is what determines whether it can actually run inline on a production network. The false positive rate is the other number that gets underreported. In operational environments, alert fatigue is a real problem, and an IDS that triggers too many false alarms tends to get ignored or tuned into irrelevance. This paper tries to address both dimensions simultaneously. The specific contributions are: (i) a side-by-side evaluation of six ML classifiers on NSL-KDD using four metrics; (ii) a simple latency-tier grouping to guide deployment choices; and (iii) a set of techniques for reducing false positives without gutting recall.

LITERATURE REVIEW.

The survey by Buczak and Guven [1] remains one of the more comprehensive overviews of ML-based IDS methods, covering more than 40 algorithms across multiple datasets. Their central observation — that ensemble methods generally outperform single classifiers in both accuracy and noise robustness — has held up reasonably well in subsequent work, and it shaped the decision to include both standalone and ensemble models in this study.

Tavallaee et al. [2] pointed out some significant statistical problems with the original KDD Cup 1999 dataset, including a large proportion of duplicate records that caused models to appear more accurate than they actually were. Their corrected version, NSL-KDD, removed those duplicates and has since become the standard benchmark in the field. Crucially, they also documented the severe under-representation of U2R and R2L samples — an issue that directly affects how any classifier performs on those categories, and one we had to deal with explicitly in our experimental setup.

Shone et al. [3] took a different approach by building a non-symmetric deep autoencoder (NDAE) for anomaly detection, reporting 97.85% accuracy on NSL-KDD. The architecture is appealing because it does not require attack labels during training. One limitation of their work, however, is that inference latency is not discussed, which makes it difficult to judge whether the model is viable for real-time inspection. This paper attempts to fill in that gap, at least partly, by measuring latency for an autoencoder configuration under comparable hardware conditions.

The Isolation Forest algorithm [5] takes a conceptually different route: rather than modelling what normal data looks like, it tries to isolate anomalies directly by partitioning the feature space at random. Because anomalies tend to occupy sparse

ISSN 3030-3907

regions, they get isolated in fewer steps. The practical consequence is that Isolation Forest can be very fast — sub-5 ms inference is achievable — and it does not require labelled training data, which is a genuine advantage in environments where attack samples are scarce.

XGBoost [7] was not originally designed with network security in mind; it was built for structured prediction tasks in domains like finance and search ranking. That said, its combination of gradient-boosted trees, built-in regularisation, and efficient parallelisation has made it a strong performer across many tabular classification problems. Whether it translates equally well to real-time IDS — especially when latency is constrained — is something this paper examines directly.

RESEARCH METHODOLOGY.

Dataset and Preprocessing

All experiments used the NSL-KDD dataset, which contains 125,973 training and 22,544 test records across five classes: Normal, DoS, Probe, U2R, and R2L. Categorical features — protocol_type, service, and flag — were encoded with one-hot encoding; numerical features were min-max normalised to [0, 1]. The class imbalance in U2R (only 231 training samples) and R2L (1,126 samples) was addressed by applying SMOTE solely to the training split, bringing each minority class up to 3,000 synthetic samples [2]. It is worth noting that SMOTE was deliberately kept out of the test set to avoid inflating evaluation metrics.

Feature Selection

The original NSL-KDD feature set has 41 attributes. Not all of them carry equal predictive weight, and including noisy or redundant features tends to hurt both generalisation and speed. We first dropped any feature whose Mutual Information score with the target fell below 0.01, then applied Recursive Feature Elimination (RFE) using XGBoost as the base estimator to narrow the set further. The resulting 25 features cut training time by around 34% and lifted mean F1-score by roughly 0.03 across classifiers — a modest but consistent improvement [1].

Algorithm Configuration

Six classifiers were included. Isolation Forest was configured with 200 estimators and contamination set to 0.05. The Autoencoder used a symmetric encoder-decoder with hidden layers of sizes [128, 64, 32], trained for 50 epochs using the Adam optimiser. XGBoost was set to 300 trees, maximum depth of 6, learning rate 0.1, and row subsampling of 0.8. Random Forest used 200 trees with the square-root feature subset rule. SVM used an RBF kernel with C=10 and gamma='scale'. Finally, a two-layer Bidirectional LSTM with 128 units per layer

ISSN 3030-3907

and 0.3 dropout was included to represent sequence-aware deep learning. All models were built in Python 3.10 with scikit-learn 1.3 and TensorFlow 2.13.

Evaluation Protocol

Five-fold stratified cross-validation was used throughout. The reported metrics are macro-averaged accuracy, F1-score, false positive rate (FPR), and mean inference latency. Latency was measured over 10,000 sequential prediction calls on a single CPU core (Intel Core i7-12700 at 3.6 GHz) — a deliberate choice to reflect deployment scenarios where GPU resources may not be available. Pairwise accuracy differences were tested for statistical significance using the Wilcoxon signed-rank test at $\alpha = 0.05$.

RESULTS AND DISCUSSION.

Overall Performance Comparison

Table 1 shows the macro-averaged results for all six models. XGBoost comes out ahead on both accuracy (around 97–99%) and inference speed (under 3 ms), which is a combination that is hard to ignore for real-time applications. Random Forest is the next closest, sitting in the 95–97% accuracy range with acceptable latency. Isolation Forest trails on accuracy at 92–94%, but it is worth remembering that it requires no labels during training — a meaningful practical advantage that the raw accuracy figure does not capture.

1-jadval

Comparative performance of ML algorithms on NSL-KDD [1–7]

№	Algorithm	Accuracy (%)	F1-Score	Latency	False Positive (%)
1	Isolation Forest	92–94	0.91	Low (≤5 ms)	5–8
2	Autoencoder (Deep)	93–96	0.93	Medium (5–15 ms)	4–6
3	XGBoost	97–99	0.97	Low (≤3 ms)	1–3
4	Random Forest	95–97	0.95	Medium (4–10 ms)	2–4
5	SVM	88–92	0.88	High (>15 ms)	6–10
6	LSTM (RNN)	94–97	0.95	High (>20 ms)	3–5

Latency Tier Analysis

ISSN 3030-3907

Looking at the latency figures, three tiers emerge fairly naturally. XGBoost and Isolation Forest both sit below 5 ms and can realistically run on low-power ARM devices without any GPU assistance — useful for edge or embedded deployments. Random Forest and the Autoencoder land in the 5–15 ms band; not ideal for the tightest latency budgets, but workable, and GPU acceleration brings the Autoencoder well below 5 ms in practice. SVM and LSTM are a different story: both exceed 15 ms, and LSTM can push past 20 ms. This is not a problem if the goal is periodic traffic analysis or post-incident forensics, but inline real-time inspection becomes difficult at those speeds [5].

Per-Category Detection Analysis

DoS detection was straightforward for tree-based models — recall exceeded 99% consistently, which is expected given the distinctive high-volume patterns these attacks generate. Probe attacks proved somewhat trickier; XGBoost and LSTM both reached F1 above 0.94, likely because they capture higher-order feature interactions and temporal patterns that simpler models miss. U2R and R2L were, as anticipated, the hardest categories. Before SMOTE, XGBoost's F1 on U2R sat at 0.48 — essentially poor, given that random guessing on a heavily imbalanced set could approach that. After applying SMOTE to the training data, the same model reached 0.79, which is a substantial jump and underlines just how much the class imbalance was suppressing performance [2][4].

False Positive Reduction

Four approaches were tested in combination. Feature selection alone brought FPR down by about 31% across the board — a fairly clean win with no real downside. Threshold optimisation using the Youden index on the validation ROC curve added another 22% reduction, though this came at the cost of a 4% drop in recall, which may or may not be acceptable depending on the deployment context. The most aggressive reduction came from the cascade setup: Isolation Forest pre-filtering traffic and passing flagged samples to XGBoost for re-scoring produced a combined FPR of 1.2% — roughly 58% lower than running XGBoost alone — while keeping total latency under 5 ms [5][7]. SMOTE, interestingly, improved minority-class recall without meaningfully changing FPR for the majority class, which suggests the two optimisation axes are largely independent and can be pursued simultaneously.

CONCLUSION AND RECOMMENDATIONS.

This study set out to compare six machine learning classifiers for network intrusion detection across four performance dimensions — accuracy, F1-score, inference latency, and false positive rate — using the NSL-KDD dataset as a common testbed. The results are reasonably clear, at least for the top performers.

ISSN 3030-3907

XGBoost is the most practical choice for real-time deployment: it delivers strong accuracy, keeps latency well below the 5 ms threshold, and is amenable to false-positive reduction through threshold tuning. Isolation Forest sits in an interesting secondary role — lower raw accuracy, but fully unsupervised and fast enough for edge hardware, making it a natural fit for environments where labelled data is scarce or where catching unknown attack patterns takes priority.

LSTM-based models are in a different category. Their sequential architecture makes them good at picking up time-dependent attack patterns, but the latency cost is real and rules them out for inline inspection in most settings. They are better suited to scheduled batch analysis or threat-hunting workflows where the analyst has time to work through flagged traffic in depth.

In terms of practical recommendations, teams looking to reduce false positives should treat the problem as multi-layered: start with SMOTE during training to handle class imbalance, calibrate the decision threshold against a validation set using the Youden index, and if resources allow, add a two-stage Isolation Forest + XGBoost cascade at inference time. Periodic model updates are also worth building into the pipeline — traffic distributions shift over time, and a model that was well-calibrated six months ago may have drifted.

Future directions worth exploring include federated learning configurations that let organisations share detection models without exposing raw traffic data, explainable AI tools that would make it easier for analysts to understand why a specific alert was triggered, and hardware-level implementations of XGBoost inference on FPGAs, which could plausibly bring latency below 1 ms at line rate [6][7].

REFERENCES

1. 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. — P. 1153–1176.
2. Tavallaee M., Bagheri E., Lu W., Ghorbani A. A detailed analysis of the KDD CUP 99 data set // Proc. IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA). — Ottawa, Canada. — 2009. — P. 1–6.
3. Shone N., Ngoc T. N., Phai V. D., Shi Q. A deep learning approach to network intrusion detection // IEEE Transactions on Emerging Topics in Computational Intelligence. — 2018. — Vol. 2, No. 1. — P. 41–50.
4. Agrawal S., Agrawal J. Survey on anomaly detection using data mining techniques // Procedia Computer Science. — 2015. — Vol. 60. — P. 708–713.

ISSN 3030-3907

5. Liu F. T., Ting K. M., Zhou Z. H. Isolation Forest // Proc. 8th IEEE International Conference on Data Mining (ICDM). — Pisa, Italy. — 2008. — P. 413–422.
6. An J., Cho S. Variational autoencoder based anomaly detection using reconstruction probability // Special Lecture on IE. — Seoul, South Korea. — 2015. — Vol. 2, No. 1. — P. 1–18.
7. Chen T., Guestrin C. XGBoost: A scalable tree boosting system // Proc. 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. — San Francisco, USA. — 2016. — P. 785–794.

ISSN 3030-3907