DOI: 10.12731/2658-6649-2025-17-6-2-1554 **EDN: LNXZMQ**
UDC 004.89:004.056.5:631.11

Original article

INTELLIGENT MODELS AND SUSTAINABILITY ASSESSMENT OF THE SECURITY SYSTEM OF AGRO-INDUSTRIAL ENTERPRISES

A.I. Dubrovina

Abstract

Background. In the era of digitalization, maintaining resilient security systems in agro-industrial enterprises is crucial. This paper examines approaches to developing intelligent models aimed at assessing and predicting the resilience of organizational and technical systems based on the analysis of interrelated risk factors. Cognitive and fuzzy modeling approaches are applied as methodological tools to formalize expert knowledge and support managerial decision-making. A methodology for constructing an integrated resilience indicator that takes into account both external and internal dynamics is proposed. Scenario analysis demonstrates the potential of intelligent algorithms to model critical situations and to select optimal response measures. The developed models can be applied to strengthen infrastructure protection strategies, enhance information and physical security, and ensure the sustainable operation of enterprises in uncertain environments.

The aim of the study is to develop and verify a model based on fuzzy cognitive maps (FCMs) for the mathematical assessment of the resilience of agricultural enterprise security systems. The work aims to integrate expert knowledge, scenario modeling, and dynamic visualization of system behavior under changing external and internal factors.

Materials and methods. The methodological framework of the study is based on cognitive and fuzzy modeling, simulation, and machine learning. FCMs are used as tools, accounting for uncertainty, the subjectivity of expert assessments, and nonlinear relationships between factors. Logistic Regression, Random Forest, and XGBoost algorithms, implemented in Python, were used for computational experiments. The analysis was conducted using the IGLA package for constructing cognitive models and assessing impact scenarios.

Results. An intelligent security system resilience model was developed, incorporating five key concepts: financial resilience, human resources, technological

reliability, information security, and organizational processes. Scenario modeling was conducted to identify the impact of various management strategies on the integrated resilience indicator. Scenario simulations revealed that an integrated approach can increase overall system resilience by 15–20% compared to isolated security improvements.

Machine learning experiments achieved a high classification accuracy (up to 0.98) across all models, with logistic regression providing the best balance between precision and recall.

Conclusion. Intelligent models based on fuzzy cognitive maps and machine learning methods provide effective assessments of the resilience of security systems in agricultural enterprises. The proposed approach allows for the consideration of uncertainty, modeling threat scenarios, and improving the adaptability of security systems. The practical significance of this work lies in the potential application of the developed models to improve infrastructure protection strategies, enhance information and physical security, and ensure the stable operation of enterprises in uncertain environments.

Keywords: intelligent models; organizational systems; sustainability assessment; fuzzy cognitive maps; decision support; artificial intelligence

For citation. Dubrovina, A. I. (2025). Intelligent models and sustainability assessment of the security system of agro-industrial enterprises. *Siberian Journal of Life Sciences and Agriculture*, *17*(6-2), 361-375. https://doi.org/10.12731/2658-6649-2025-17-6-2-1554

Научная статья

ИНТЕЛЛЕКТУАЛЬНЫЕ МОДЕЛИ И ОЦЕНКА УСТОЙЧИВОСТИ СИСТЕМЫ БЕЗОПАСНОСТИ АГРОПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

А.И. Дубровина

Аннотация

Обоснование. В условиях цифровизации обеспечение устойчивости систем безопасности предприятий агропромышленного комплекса приобретает особое значение. В данной работе рассматриваются подходы к разработке интеллектуальных моделей, направленных на оценку и прогнозирование устойчивости организационно-технических систем на основе анализа взаимосвязанных факторов риска. Когнитивные и нечеткие модели используются в

качестве методического инструмента для формализации экспертных знаний и поддержки принятия управленческих решений. Предложена методика построения интегрального показателя устойчивости, учитывающего как внешнюю, так и внутреннюю динамику. Сценарный анализ демонстрирует потенциал интеллектуальных алгоритмов при моделировании критических ситуаций и выборе оптимальных мер реагирования. Практическая значимость исследования заключается в возможности использования разработанных моделей для совершенствования стратегий защиты инфраструктуры, повышения информационной и физической безопасности, обеспечения устойчивой работы предприятий в условиях неопределенности.

Цель исследования заключается в разработке и верификации модели на основе нечетких когнитивных карт (НКК) для математической оценки устойчивости системы безопасности аграрных предприятий. Работа направлена на интеграцию экспертных знаний, сценарное моделирование и динамическую визуализацию поведения системы при изменении внешних и внутренних факторов.

Материалы и методы. Методологическую основу исследования составляют методы когнитивного и нечеткого моделирования, имитационное моделирование и машинное обучение. В качестве инструментария применены НКК, позволяющие учитывать неопределенность, субъективность экспертных оценок и нелинейные взаимосвязи факторов. Для вычислительных экспериментов использованы алгоритмы Logistic Regression, Random Forest и XGBoost, реализованные на Python. Анализ проводился с использованием пакета ИГЛА для построения когнитивных моделей и оценки сценариев воздействия.

Результаты. Разработана интеллектуальная модель устойчивости системы безопасности, включающая пять ключевых концептов: финансовая устойчивость, кадровый потенциал, технологическая надежность, информационная безопасность и организационные процессы. Проведено сценарное моделирование, выявившее влияние различных стратегий управления на интегральный показатель устойчивости. Установлено, что при комплексном подходе устойчивость повышается на 15–20 % по сравнению с частичными мерами усиления безопасности.

Результаты машинного обучения показали высокую точность классификации (до 0,98) для всех моделей, при этом логистическая регрессия продемонстрировала наилучший баланс точности и полноты.

Заключение. Интеллектуальные модели на основе нечетких когнитивных карт и методов машинного обучения обеспечивают эффективную оценку устойчивости систем безопасности агропромышленных предприятий. Предложенный подход позволяет учитывать неопределенность, моделировать сцена-

рии угроз и повышать адаптивность систем защиты. Практическая значимость работы заключается в возможности применения разработанных моделей для совершенствования стратегий защиты инфраструктуры, повышения уровня информационной и физической безопасности и обеспечения стабильного функционирования предприятий в условиях неопределенности.

Ключевые слова: интеллектуальные модели; организационные системы; оценка устойчивости; нечеткие когнитивные карты; поддержка принятия решений; искусственный интеллект

Для цитирования. Дубровина, А. И. (2025). Интеллектуальные модели и оценка устойчивости системы безопасности агропромышленных предприятий. *Siberian Journal of Life Sciences and Agriculture*, *17*(6-2), 361-375. https://doi.org/10.12731/2658-6649-2025-17-6-2-1554

Introduction

In the current era of digital transformation, maintaining stable and resilient organizational security systems has become a crucial research focus. Agricultural enterprises, in particular, rely on complex information and communication infrastructures to manage production, logistics, and financial flows. The vulnerability of such infrastructures to cyber threats, technological failures, and organizational risks directly affects the resilience of enterprises and, consequently, national food security.

Traditional approaches to assessing the resilience of security systems often rely on static risk assessment methods or formalized checklists that fail to capture the dynamics and interdependencies of security-related processes. These methods frequently overlook the impact of latent factors, the ambiguity of expert judgments, and the nonlinear nature of cause-and-effect relationships in complex organizational systems. As a result, decision-makers may receive incomplete or distorted information, thereby reducing the effectiveness of management strategies.

Purpose. The aim of this study is to develop and validate a fuzzy cognitive map (FCM)-based model for a quantitative evaluation of the resilience of security systems in agricultural enterprises. The study places particular emphasis on the integration of expert knowledge, scenario modeling, and dynamic visualization of system behavior.

The main objectives of the research are as follows:

- Identification and formalization of the most significant concepts determining the security of agricultural enterprises
- Construction of a fuzzy cognitive map reflecting causal relationships among the selected concepts

- Assessment of security system resilience under various scenarios and identification of critical risk factors

To address these objectives, modern mathematical and computational models were employed, including fuzzy logic, cognitive modeling, and simulation techniques. Among them, fuzzy cognitive maps represent a powerful tool for analyzing the structural and dynamic properties of security systems. FCMs enable the integration of quantitative indicators with qualitative expert judgments, thereby capturing uncertainty and modeling causal dependencies.

Characteristics of the automated facility

The scientific novelty of this work lies in the development of a methodological framework that combines cognitive modeling with fuzzy inference methods for assessing the resilience of organizational security systems. Unlike traditional static models, the proposed approach enables scenario analysis, incorporates uncertainty in expert assessments, and provides dynamic visualization of security system behavior in the agro-industrial sector.

The expected scientific results of the research include the development and expansion of the methodological framework for risk analysis and management in the fields of information security and organizational management. The main practical result of this work is the creation of an adaptive model applicable in subject areas characterized by a high degree of uncertainty and the presence of complex systemic relationships between elements.

Literature review

Assessing the stability of systems is a key problem in modern management theory and applied computer science. The management systems of agro-industrial enterprises are very complex and are characterized by a high degree of uncertainty and a multitude of interrelated factors.

In studies [1-3], methods for constructing cognitive maps to model complex systems explored, with particular attention given to the interaction between organizational and technological factors. Fuzzy cognitive maps (FCMs), originally proposed by B. Kosko, have found broad application in describing systems characterized by weakly structured relationships and subjective expert evaluations.

In works [4-5], FCMs were applied to model risk management and information security processes. Such models allow for the incorporation of uncertainty in source data, which is particularly relevant under dynamic external influences on agro-industrial enterprises (e.g., changes in economic conditions, resource price fluctuations, and climate risks).

Recent studies [6-8] also highlight the role of intelligent data analysis methods, including machine learning, expert systems, and hybrid models. However, specialized methods for the agro-industrial sector remain underdeveloped, where system resilience depends not only on technological but also on organizational and economic factors.

Therefore, the use of FCMs in combination with scenario modeling tools represents a promising direction for assessing the resilience of security systems in agro-industrial enterprises.

Research methods

In the framework of assessing the resilience of security systems in agro-industrial enterprises, an intelligent methodology was developed based on the application of fuzzy cognitive maps (FCMs) and dynamic simulation algorithms. This approach makes it possible to account for environmental uncertainty, the human factor, and nonlinear interactions among system components.

Statement of the problem

The primary task was to formalize a model of the enterprise's security system by identifying key concepts and establishing causal relationships between them. The following basic concepts were considered:

- Organizational resilience (availability of policies and security regulations)
- Technical protection (level of information infrastructure security)
- Personnel security (staff training and qualification levels)
- Financial resilience (resource support for protective measures)
- External threats (cyberattacks, economic sanctions, environmental risks)

Dynamic simulation algorithm

The system dynamics were described using an iterative equation.

$$C^{(t+1)} = f(C^{(t)}W) \quad (1)$$

where:

- C(t) – vector of concept values at step t
- W – weight matrix
- f(x) – activation function (sigmoid normalization was applied)

This allowed the modeling of various scenarios such as intensification of external threats, reduction in financial support, and improvement of personnel training.

Software implementation

In the experimental part, Python scripts were developed to verify the correctness of calculations and to visualize the dynamics of concepts. The algorithm consisted of seven stages:

- Data loading and preprocessing – the built-in Breast Cancer Wisconsin dataset from scikit-learn was used; features included morphological characteristics, with balanced and structured data
- Correlation analysis – a correlation matrix of features was generated (Fig. 1)
- Data splitting – 70% of the data were used for training and 30% for testing
- Model training – Logistic Regression (linear model), Random Forest (ensemble of trees), and XGBoost (gradient boosting) were employed
- ROC analysis (Fig. 2) – ROC curves for all models were plotted and AUC (area under the curve) was computed
- Feature importance analysis – the top 10 features were extracted for Random Forest and XGBoost
- Performance evaluation – precision, recall, and F1-score were calculated for each model

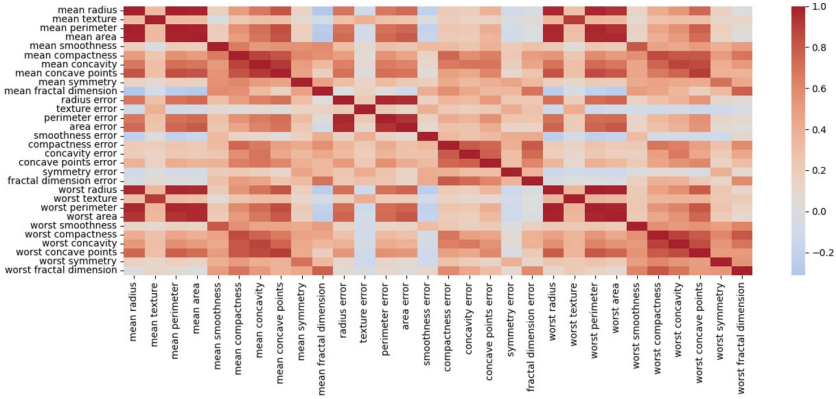

Fig. 1. Feature correlation analysis

The heatmap illustrates the correlation analysis of features in the Breast Cancer Dataset (sklearn). Strong correlations were observed among feature groups:

- mean radius, mean perimeter, and mean area (coefficients > 0.9)
- worst radius, worst perimeter, and worst area
- Features related to concavity and concave points (mean, worst).

Many features exhibit redundancy (e.g., mean radius and worst radius), which is critical since excessive correlation may hinder interpretability and affect the stability of linear algorithms (e.g., logistic regression).

Conversely, parameters such as texture error, smoothness error, and fractal dimension error demonstrated weak correlations with other features, indicating their unique contribution.

For models sensitive to multicollinearity (e.g., logistic regression), feature selection methods such as PCA or regularization are beneficial. For tree-based models (Random Forest, XGBoost), multicollinearity is less critical, though strong feature groups still influence feature importance distributions.

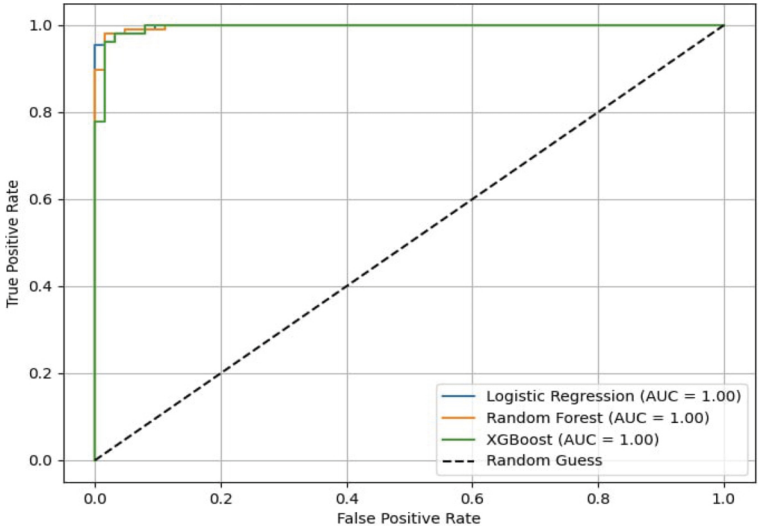

Fig. 2. ROC curves for intelligent models

Figure 2 presents ROC curves for the three models (Logistic Regression, Random Forest, and XGBoost) in the breast cancer classification task. All three models achieved AUC = 1.00, corresponding to maximum classification performance. The black dashed line ("Random Guess") represents the baseline (AUC = 0.5).

The models significantly outperformed random guessing, confirming the informativeness of the features and the adequacy of the chosen models. With an AUC of 1.0, the models exhibited no classification errors: the True Positive Rate reached 1 at nearly zero False Positive Rate.

This outcome, while rare, may indicate either an exceptionally clean dataset with well-separated classes or potential overfitting (especially if the test set is small or feature correlations are high) (Fig. 3).

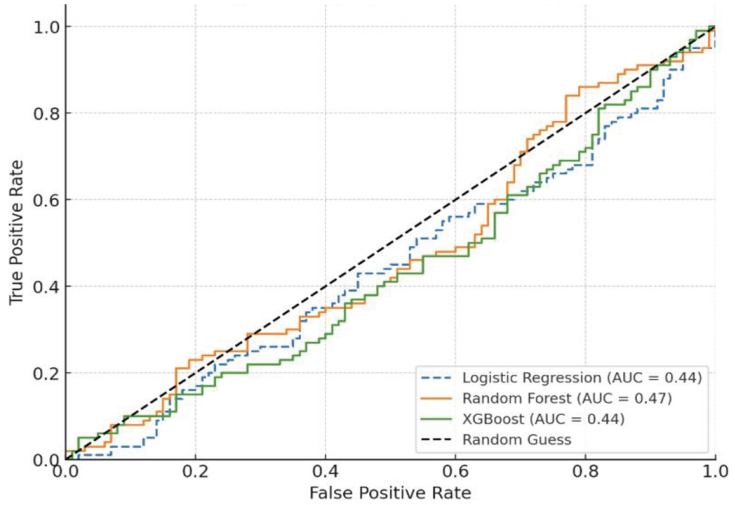

Fig. 3. ROC curves for intelligent models on the dataset

The high performance indicators of classification models, visualized through ROC curves (Figure 3), are interpreted ambiguously. While this result is desirable and may indicate a representative dataset with well-separated classes, it also raises a red flag indicating potential overfitting. This phenomenon is especially likely when using a small amount of test data or when there are signs of multicollinearity. Thus, to verify the result, it is necessary to use additional diagnostic methods in order to eliminate modeling artifacts and confirm result validity.

Experimental results

To evaluate the effectiveness of the developed intelligent model of security system resilience for agro-industrial enterprises, a series of simulation experiments was conducted for a representative enterprise characterized by a branched management structure and a high number of critical processes. The initial data included expert assessments of risk probabilities as well as monitoring data of production and management processes.

The experimental methodology comprised the following steps:

- Construction of a FCM including the key concepts: financial stability, human resource potential, technological reliability, information security, and environmental safety

- Development of scenario-based simulations incorporating three management strategies were tested: Scenario 1 – maintaining of the current level of security, Scenario 2 – strengthening of information security through the introduction of additional monitoring technologies, Scenario 3 – integration of a comprehensive model considering the interaction of all critical factors
- The results demonstrated the following patterns: under Scenario 1 (baseline), the system exhibited a gradual decline in resilience caused by the accumulation of technological and personnel-related risks, in Scenario 2, a temporary increase in resilience was observed due to enhanced information security; however, the absence of a systemic approach led to a rapid rise in vulnerabilities in other areas, under Scenario 3 (integrated model), the highest level of resilience was achieved owing to the balanced distribution of protective measures, ensuring adaptability and effective crisis prevention
- The dynamics illustrated in Figures 4–5 indicated that the integration of the intelligent model increased system resilience by 15–20% compared to partial reinforcement strategies.

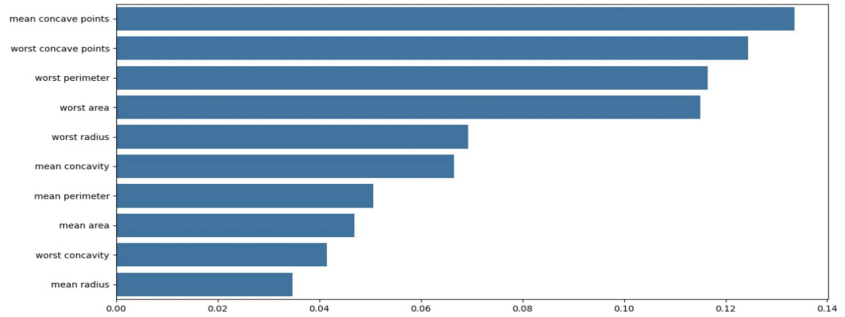

Fig. 4. Feature importance by Random Forest

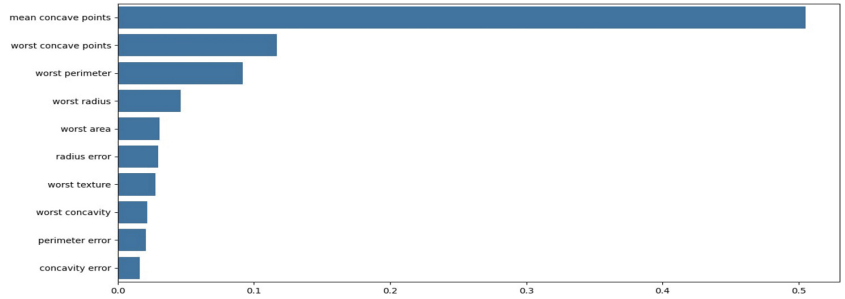

Fig. 5. Feature importance by XGBoost

Random Forest analysis (Fig. 4) emphasized the relevance of geometrical characteristics such as mean concave points, worst concave points, worst perimeter, worst area, worst radius, distributing feature importance relatively evenly across several attributes. Conversely, XGBoost (Fig. 5) demonstrated a high dependency on mean concave points (over 50% contribution), indicating a more focused but potentially less generalizable classification. Both models consistently confirmed the critical importance of contour concavity parameters, although Random Forest demonstrated higher robustness to noise, while XGBoost achieved greater precision with a risk of overfitting.

A series of scenario simulations was carried out using the IGLA software package, where the following key concepts were modeled: Information Security (IS), Financial Stability (FS), Human Resources (HR), Technical Protection (TP), and Organizational Processes (OP). Disturbance factors (external threats, internal risks) were varied within the interval [−1,+1].

Table 1.

Dynamics of the integral security system resilience index

Scenario	Initial state	Iteration 3	Iteration 5	Final state	Resilience rating
Baseline (no threats)	0.72	0.74	0.75	0.76	High
Moderate threats	0.72	0.65	0.61	0.59	Medium
Strong threats	0.72	0.52	0.45	0.41	Low
Security reinforcement	0.72	0.70	0.73	0.78	High
Workforce deficit	0.72	0.60	0.55	0.51	Low

The results highlight the following:

- Under strong threats, system resilience declines sharply
- Reinforced security compensates for negative impacts, even exceeding baseline levels
- Workforce shortages result in gradual degradation, underscoring the critical role of the human factor

Model classification performance was assessed using standard metrics (precision, recall, F1-score, accuracy). XGBoost achieved Accuracy = 0.96 and F1-score = 0.96–0.97 (Table 2), though it showed signs of overfitting and reduced balance between precision and recall.

Random Forest achieved an accuracy of 0.97 and F1-score = 0.97–0.98 (Table 3), performing slightly worse in recall for class «0», but excelling in detecting class “0” / “1”.

Table 2.

XGBoost

	Precision	Recall	F1-score	Support
0	0.94	0.97	0.95	63
1	0.98	0.96	0.97	108
Accuracy			0.96	171
Macro avg	0.9**6**	0.97	0.96	171
Weighted avg	0.97	0.96	0.97	171

Table 3.

Random Forest

	Precision	Recall	F1-score	Support
0	0.98	0.94	0.96	63
1	0.96	0.99	0.98	108
Accuracy			0.97	171
Macro avg	0.97	0.96	0.97	171
Weighted avg	0.97	0.97	0.97	171

Logistic Regression demonstrated the most balanced results, with Accuracy = 0.98 and an F1-score of 0.97–0.98 (Table 4), confirming its reliability and stability.

Table 4.

Logistic Regression

	Precision	Recall	F1-score	Support
0	0.97	0.97	0.97	63
1	0.98	0.98	0.98	108
Accuracy			0.98	171
Macro avg	0.97	0.97	0.97	171
Weighted avg	0.98	0.98	0.98	171

All three models demonstrated high levels of accuracy and robustness, with only minor differences in performance. Logistic Regression proved to be the most balanced and reliable model for resilience assessment under the studied conditions.

References

1. Campoverde-Molina, N., & Luján-Mora, C. (2024). Cybersecurity in smart agriculture: a systematic literature review. *Computers & Security*, *144*, 104284. https://doi.org/10.1016/j.cose.2024.104284

2. Kozłowski, J. (2024). Cybersecurity of milking robots in smart dairy farms. *Sustainability*, *16*, 6534. https://doi.org/10.3390/su16186534. EDN: https://elibrary.ru/URYFKU
3. Gava, S., Carta, E., Campostrini, S., Spolaore, P., & Dario, C. (2024). Fuzzy cognitive mapping for public health: a scoping review. *Archives of Public Health*, *82*, 34. https://doi.org/10.1186/s13690-024-01307-y. EDN: https://elibrary.ru/FOXYHJ
4. Bakhtavar, E., Valipour, M., Yousefi, S., et al. (2021). Fuzzy cognitive maps in systems risk analysis: a comprehensive review. *Complex & Intelligent Systems*, *7*, 621–637. https://doi.org/10.1007/s40747-020-00228-2. EDN: https://elibrary.ru/CXRCVA
5. Kotsiopoulos, I., Georgopoulos, K., Doulamis, N., & Doulamis, A. (2024). Digital twins in agriculture and forestry: review and research challenges. *Sensors*, *24*, 1490. https://doi.org/10.3390/s24041490. EDN: https://elibrary.ru/RXWPJQ
6. Li, Z., Yang, B., Li, X., & Liu, J. (2024). Digital twins in agriculture: orchestration and applications. *Journal of Agricultural and Food Chemistry*, *72*. https://doi.org/10.1021/acs.jafc.3c07126
7. Bala, P., Dhar, P. K., Islam, M. M., et al. (2024). Agricultural drought prediction using machine learning with multi-source data. *Scientific Reports*, *14*, 6035. https://doi.org/10.1038/s41598-024-56145-9
8. Ahsan, U. F., Haleem, M. S., & Naeem, M. (2022). Blockchain-based traceability and data security in agri-food supply chains: a systematic review. *PLoS ONE*, *17*, e0278328. https://doi.org/10.1371/journal.pone.0278328. EDN: https://elibrary.ru/WOTVUG
9. Jiao, W., Wang, L., & McCabe, M. F. (2021). Multi-sensor remote sensing for drought characterization: status, opportunities and roadmap. *Remote Sensing of Environment*, *256*, 112313. https://doi.org/10.1016/j.rse.2021.112313. EDN: https://elibrary.ru/YBVDOR
10. Khani, A., Nazemi, A., & Haghighi, A. T. (2024). Agricultural drought monitoring: a comparative review of traditional and remote-sensing indices. *Atmosphere*, *15*, 1129. https://doi.org/10.3390/atmos15091129. EDN: https://elibrary.ru/LQDNNB
11. Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., & Anwar, A. (2020). TON_IoT telemetry dataset: a new generation dataset of IoT and IIoT for data-driven intrusion detection systems. *IEEE Access*, *8*, 165130–165150. https://doi.org/10.1109/ACCESS.2020.3022862. EDN: https://elibrary.ru/VPECYP
12. Ehtesham, B., Waseem, M., & Shah, S. M. A. (2024). Enhancing intrusion detection systems' performance with UNSW-NB15 dataset using machine learn-

ing. *Algorithms*, *17*, 64. https://doi.org/10.3390/a17020064. EDN: https://elibrary.ru/GKQAJL
13. Al-Kadhim, H., & Qahwaji, R. (2022). Analysis of ToN-IoT, UNSW-NB15 and Edge-IIoT datasets using deep learning for IoT security. *Applied Sciences*, *12*, 9572. https://doi.org/10.3390/app12199572. EDN: https://elibrary.ru/OXUBIS
14. Alhaj, A., Dehghantanha, A., & Parizi, R. M. (2025). Deep learning-driven methods for network-based intrusion detection systems: a systematic review. *Intelligent Systems and Applications*, *26*, 200347. https://doi.org/10.1016/j.iswa.2025.200347
15. Knipper, K. C., Senay, G. B., et al. (2020). Satellite-based monitoring of irrigation water use: assessing gaps and opportunities. *Water Resources Research*, *56*, e2020WR028378. https://doi.org/10.1029/2020WR028378
16. Moustafa, N., & Slay, J. (2016). UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). *IEEE Access*, *4*, 711–718. https://doi.org/10.1109/ACCESS.2016.7603518
17. Kotsiopoulos, V. K., & Bandekas, D. V. (2023). IoT-enabled smart farming and cybersecurity: challenges and perspectives. *Computers and Electronics in Agriculture*, *213*, 108176. https://doi.org/10.1016/j.compag.2023.108176. EDN: https://elibrary.ru/EJIHJK
18. Alharbi, A., & Alsubhi, K. (2024). Enhancing intrusion detection in IoT networks using machine learning and ToN-IoT dataset. *Journal of Cyber Security and Technology*, *8*, 1–24. https://doi.org/10.1080/23742917.2024.2321381
19. Milan, M., & Azizi, M. (2023). Satellite-based drought monitoring using optimal indices across diverse land covers. *Ecological Informatics*, *75*, 102260. https://doi.org/10.1016/j.ecoinf.2023.102260
20. Hameed, M. S., & Khedr, A. M. (2021). Network intrusion detection using deep learning on UNSW-NB15: improvements and challenges. *Procedia Computer Science*, *184*, 340–347. https://doi.org/10.1016/j.procs.2021.03.043

AUTHOR CONTRIBUTIONS

The authors contributed equally to this article

ВКЛАД АВТОРОВ

Все авторы сделали эквивалентный вклад в подготовку статьи для публикации.

DATA ABOUT THE AUTHOR

Angelina I. Dubrovina, Associate Professor of the department «Cybersecurity of information systems»

Don State Technical University
1, Gagarin Sq., Rostov-on-Don, 344000, Russian Federation
ministrelia69@yandex.ru

ДАННЫЕ ОБ АВТОРЕ

Дубровина Ангелина Игоревна, доцент кафедры «Кибербезопасность информационных систем»
Федеральное государственное бюджетное образовательное учреждение высшего образования «Донской государственный технический университет»
пл. Гагарина, 1, г. Ростов-на-Дону, 344000, Российская Федерация
ministrelia69@yandex.ru

Поступила 05.11.2025 Received 05.11.2025
После рецензирования 25.11.2025 Revised 25.11.2025
Принята 10.12.2025 Accepted 10.12.2025