UDC 004.8 **doi:** https://doi.org/10.20998/2522-9052.2024.1.11

Oleksandr Shefer[1], Oleksandr Laktionov[1], Volodymyr Pents[1], Alina Hlushko[1], Nina Kuchuk[2]

[1] National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine
[1] National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

PRACTICAL PRINCIPLES OF INTEGRATING ARTIFICIAL INTELLIGENCE INTO THE TECHNOLOGY OF REGIONAL SECURITY PREDICTING

Abstract. Objective. The aim is to enhance the efficiency of diagnostics for determining the level of air attack safety through the practical integration principles of artificial intelligence. **Methodology.** Models and technologies for safety diagnostics of the region (territorial community) have been explored. The process of building an artificial intelligence model requires differentiation of objects at a level to accumulate assessments-characteristics of aerial vehicles. The practical integration principles of artificial intelligence into the forecasting technology are based on the Region Safety Index, used for constructing machine learning models. The optimal machine learning model of the proposed approach is selected from a list of several models. **Results.** A technology for predicting the level of regional safety based on the Safety Index has been developed. The recommended optimal model is the Random Forest model ([('max_depth', 13), ('max_features', 'sqrt'), ('min_samples_leaf', 1), ('min_samples_split', 2), ('n_estimators', 79)]), demonstrating the most effective quality indicators of MAE; MAX; RMSE 0.005; 0.083; 0.0139, respectively. **Scientific Novelty.** The proposed approach is based on a linear model of the Region Safety Index, which, unlike existing ones, takes into account the interaction of factors. This allows for advantages of the proposed method over existing approaches in terms of the root mean square error of 0.496; 0.625, respectively. In turn, this influences the quality of machine learning models. **Practical Significance.** The proposed solutions are valuable for diagnosing the level of safety in the region of Ukraine, particularly in the context of air attacks.

Keywords: predicting; linear equation; double interaction; linear scaling; safety index.

Introduction

The analysis of the legal framework of the country, in particular the Law of Ukraine "On National Security of Ukraine", indicates the need for research updates in the development of new approaches to planning or predicting in the field of national security [1]. A number of scientific studies on predicting the security component using artificial intelligence tools are increasing each year, as evidenced by Google Trends search queries. In particular, general issues of using artificial intelligence in national security systems are discussed in detail in article [2]. Article [3] discusses the use of artificial intelligence for the environmental safety of the state. Articles [4, 5] discuss the use of the Internet of things in national security systems. Articles [6, 7] focus on data mining. The book [8] examines the implications of technical, legal, ethical, privacy, human rights and civil liberties issues regarding artificial intelligence and national security. In articles [9, 10], the emphasis is on the economic aspects of the problem under consideration. The information component of the problem under consideration is analyzed in articles [11, 12]. Aspects of the fight against complex cybercrimes are discussed in articles [13, 14]. Issues of using neural networks in research related to national security are discussed in articles [15, 16]. Aspects of the use of cloud technologies related to this problem are discussed in articles [17–19].

The effectiveness of predicting regional security, especially in terms of air defense, depends on the threat environment, tactics, and capabilities of the adversary [20]. Limitations of existing approaches to integrating artificial intelligence into regional security predicting lie in addressing a series of specific issues. Therefore, the problem is partially resolved and requires the development of new approaches.

The aim of the research is to enhance the efficiency of air attack risk diagnosis by utilizing practical principles of artificial intelligence integration.

The research focuses on the intellectual analysis process in predicting the security level of a region during air alarms.

The subject of the study includes models and information technologies for diagnosing the security of the region (territorial community).

The research tasks are as follows:

1. Conduct a comparative analysis of existing approaches to diagnosing levels of air threat complexity and propose a state security index that considers the principles of interdependence of variables, linear scaling, and exhaustive consideration of all combinations of assessments.

2. Propose a technology for predicting the level of regional security (territorial community) based on the regional security index and machine learning models.

3. Perform experimental verification of the proposed approaches.

A review of related scientific publications. Existing developments in the field of regional or national security technologies are dedicated to the development of new approaches for diagnosing and monitoring various types of threats, including ecological-economic [21], informational [22], and financial [23].

Alongside these efforts, a series of public alert systems have been developed, particularly for radiological emergencies, providing reliable information in near-real-time about the radiological status of the environment around nuclear power plants [24]. These systems are focused exclusively on diagnosing the radiological condition of power plants and are not designed for household use. The use of artificial intelligence tools is the underlying technology that

allows for event prediction, including regional security events, based on trained models.

A prototype of using artificial intelligence tools for predicting danger is presented in the work [25], where a variety of artificial intelligence models are employed to detect malicious software. This approach represents a classical foundation for utilizing artificial intelligence, with further development discussed in [26].

Research [26 explores approaches to preserving human lives by creating mobile applications with danger notifications. The proposed model describing the population's reaction to notifications uses a linear model, taking into account the cumulative values of unique mobile devices and their movement time. Essentially, this proposed model serves as a safety index. Research results indicate that 35% to 45% of civilian casualties could be avoided if the population responded to application notifications.

In another scientific work [27], the use of indices is explored at a different level. A model for the effectiveness of air defense is proposed, based on determining the probable number of air threats and the ability of air defense systems to repel an airborne attack. The model considers coefficients for individual defense tools, the number of available missiles, the interaction of a particular type of equipment in one firing cycle, and the simultaneous engagement of multiple targets.

Works [26, 27] contain indices constructed using linear mathematical operations and consider unique components that have not been studied in research [28]. However, developments in [28] propose a linear model with nonlinear variables, essentially a combined or hybrid model. This model is built on the principle of factor interaction, demonstrating sufficient accuracy based on the criterion of mean square deviation within the research framework [28].

In addition to approaches using artificial intelligence models and indices that combine multiple assessments into one overall index, a technology for predicting the level of security should characterize evacuation plans or provide evacuation recommendations based on the level of received assessments. This idea has been studied during the development of population evacuation strategies, which is a key research direction in NATO countries. During evacuations, social and material-technical factors should be considered, as recommended in [29].

Therefore, each existing approach [21–29] is unique and addresses a specific problem, not specifically focused on the features of predicting the security level of a country based on safety index assessments.

Research methodology. During the research, four components were studied, where the number of possible permutations x_1, x_2, x_3, x_4 would be the product of unique values of each variable: 5·5·5·5=625. This formed the theoretical studied sample, which comprised N_1=625 events. The experimental sample involved the use of the known dataset “Massive Missile Attacks on Ukraine” [30], accumulating information about air attacks on Ukraine since October 2022. The dataset includes N_2=605 events related to air alarms, including the start/end time of the attack, missile type, launch location, launch pad, number of launched/destroyed missiles, and the information source (mostly Facebook posts).

The technology for predicting regional security involves utilizing information from the dataset regarding missile type, launch location, launch pad, and the number of launched/destroyed missiles. The toolkit for diagnosing regional security is created using an analytical method and a modeling method, with program implementation done in Python using libraries such as Sklearn, numpy, and pandas. In the experimental investigation, a comparative analysis of the proposed index determination model and an existing one [12] was conducted.

In the process of building machine learning models, a well-known model-building technology [31] was utilized. Step 1: Build basic machine learning regression models and examine performance indicators, including R^2 (coefficient of determination), RMSE (Root Mean Square Error), MAE (Mean Absolute Error), MAX (Maximum Absolute Error), and bias-variance. Step 2: Select models that do not exhibit overfitting and improve them using grid search, particularly with the scikit-optimize package and the BayesSearchCV hyperparameter optimization method. Examine the model's performance indicators. Step 3: Select the optimal model.

Formal statement of the research task. The regions of the country R are subject to air attacks by the enemy. Attacks are carried out from a set of types of unmanned aerial vehicles x_1, where x_1 categorical variable transformed into a numerical one, ranging from 1 to 5, corresponds to the set of launch methods for objects x_4, where x_4 is a categorical variable transformed into a numerical one ranging from 1 to 5. In addition, we have characteristics of the number of launched x_2 and intercepted x_3 missiles, varying from 1 to n and from 0 to n, respectively.

Propose a model K that determines the security level of a region depending on the components: type of unmanned aerial vehicle or missile x_1, number of launches x_2, number of interceptions x_3, and launch method x_4.

Model K should consider interaction principles to determine variable dependencies, linear scaling principles to transform ratings from one range to a range of 1 to 5, and complete enumeration of all rating combinations. This will allow a more precise consideration of the variable's impact on the overall level of model K.

The proposed model K is selected from the set of models M, where K_i for $i = 1, 2, \ldots, n$, subject to condition:

$$K_{opt} = \arg\min_{K_i \in} RMSE(K_i), \qquad (1)$$

where $RMSE(K_i)$ – the value of the root mean square error for the model K.

Security level assessments of the state K will be used for constructing regression models with machine learning tools. The criteria for selecting machine learning models include RMSE, MAE, and MAX.

Experimental research. The process of developing the region's security index involves the formation of input assessments, where a crucial aspect is the study of their intervals and quantity. The researched characteristics (indicators) of the dataset include the type of unmanned aerial vehicle or missile, the number of launched/hit objects, and the method of object launch.

In investigating the types of unmanned aerial vehicles or missiles and the method of launch, 35 and 43 unique names were identified, respectively. The analysis of the quantity of launched and hit missiles revealed the following values. Launched missiles vary in the range from 1 to 96, and hit ones from 0 to 75 units. To differentiate between types of aircraft and methods of object launch, certain varieties were highlighted. The quantity of launched and hit objects is recorded with the corresponding values. The determination of the Chi-square assessments is carried out using Table 1.

Table 1 – **Types of objects and scales of object differentiation at the level for accumulating assessments-characteristics of aircraft**

Object type	Assessment or quantity of units	Type or variety of object
Type of unmanned aerial vehicle or missile, x_1	1	Drones
	2	Subsonic missiles
	3	Operational-tactical missiles
	4	Hypersonic missiles
	5	Combined option (drones + missiles)
Number of launched missiles, x_2	n launched, units	From 1 to 96
Number of intercepted missiles, x_3	k intercepted, units	From 0 to 75
Launch method of the object, x_4	1	From a launch installation
	2	Using navigation
	3	From a submarine or ship
	4	From an aircraft
	5	Combined option (all listed)

Let's note that, by analogy, other characteristics may be added during the life cycle of the technology. The mentioned variables are used to determine the region's safety index, considering the principles of interaction, linear scaling, and the enumeration of possible rating combinations.

The region's safety index K can be expressed by the model (2):

$$K = x_1 + x_2 + x_3 + x_4 + (x_1 x_3) + (x_2 x_4), \quad (2)$$

where x_1 – type of unmanned aerial vehicle or missile, x_2 – number of launched missiles (from 1 to n), x_3 – number of intercepted missiles (from 0 to k), x_4 – launch method of the object.

Since the number of launched and intercepted missiles is unknown and can vary, it is necessary to transform the variables x_2 and x_3 into a five-point range. The transformation is constrained to obtain only positive ratings within the range from 0 to 5.0. Normalizing variables using Standard Scaler, Max Abs Scaler, Min Max Scaler on the theoretical sample demonstrated negative ratings, which is unacceptable for equation (2).

Therefore, we perform the transformation of x_2 and x_3 into a range from 1 to 5 using linear scaling as follows:

$$x_{i\_t} = (((5\text{-}1) \cdot (\text{current assessment } x_i\text{-}1)) / / (\text{maximum assessment } x_i\text{-}1))+1, \quad (3)$$

where x_i – object type from table 1.

The proposed procedure is universal and ensures variable flexibility. Thus, with values of x_1, x_2, x_3, x_4 equal to 1.0, the value of K_i is 6.0, and with x_1, x_2, x_3, x_4 equal to 5.0, the value of K_i is 70.0. The final formula for the region's safety index is given by equation:

$$KS = (((5\text{-}1) \cdot (\text{current assessment } K_i\text{-}1)) / (K_{i\ max}\text{-}1))+1, \quad (4)$$

where K_i – current evaluation of K_i, $K_{i\ max}$ – maximum value of K_i.

The proposed approach serves as the basis for forming a region safety predicting technology.

Block 1. The existing dataset is imported, and evaluations are accumulated using Table 2.

Table 2 – **Types of objects and scales of object differentiation at the level for accumulating assessments-characteristics of aerial vehicles**

Object Type	Assessment or quantity of units	Type or variety of object (Characteristic)
Object Type 1	1	1.1.
	2	1.2.
	3	1.3.
	4	1.4.
	5	1.5.
Object Type 2	n, units	2.1.
Object Type 3	k, units	3.1.
Object Type 4	1	4.1.
	2	4.2.
	3	4.3.
	4	Characteristic 4.4.
	5	Characteristic 4.5.

The dataset is being examined for the number of assessed values, missing values, minimum and maximum values, and unique values.

Block 2. The determination of the region safety index is carried out using formulas (2)–(4). The formula is constructed in such a way that the values of the number of launched and intercepted missiles are normalized to a five-point scale (Table 3).

Block 3. If the obtained result does not satisfy the decision-maker, a transition to Block 1 is made, where adjustments to the input assessments are performed. Otherwise, a transition to Block 4 is carried out.

Table 3 – **Results of determining the safety index**

№	x_i	KS
1	x_{i11}	KS_{11}
2	x_{i21}	KS_{21}
…	…	…
n	x_{in1}	KS_{nm}

Block 4. The determined safety index ratings are used in machine learning regression models. Performance indicators of the models without hyperparameter tuning, namely R2train/R2test, MAE, MAX, RMSE, bias and variance, are shown in Table 4.

Based on the results of the comparative analysis, one or several models are selected for a more detailed analysis.

Block 5. If the obtained result does not satisfy the decision-maker, a transition to Block 1 is made, where adjustments to the input assessments are performed. Otherwise, a transition to Block 6 is carried out.

Table 4 – **Results of investigating the performance indicators of machine learning models without hyperparameter tuning**

Researched approach	Model 1.1	Model n
R2train/R2test	R2train/R2test	R2train/R2test
MAE	MAE	MAE
MAX	MAX	MAX
RMSE	RMSE	RMSE
Bias	Bias	Bias
Variance	Variance	Variance

Block 6. A list of hyperparameters for the safety prediction model is formed for use in the BayesSearchCV method. The results of the investigations of optimized models are shown in Table 5.

Block 7. The constructed model is checked using learning curves.

Block 8. The obtained prediction result is used to determine the danger of the region, shown in Table 6.

Table 5 – **Comparative analysis of models based on region safety index evaluations, without hyperparameter tuning, and with hyperparameters**

Researched approach	Model 1 without hyperparameter settings	Model n with hyperparameter settings
R2train/R2test	Model 1.1. R2train/R2test	Model n R2train/R2test
MAE	Model 1.1. MAE	Model n MAE
MAX	Model 1.1. MAX	Model n MAX
RMSE	Model 1.1. RMSE	Model n RMSE
Bias	Model 1.1. Bias	Model n Bias
Variance	Model 1.1. Variance	Model n Variance

Table 6 – **Levels of danger in regions of the country based on the safety index values**

№	The level of the security index of the regions	Danger level of the region
1	From 1.0 to 2.0	Low level of danger
2	From 2.01 to 3.0	Medium level of danger
3	From 3.01 to 4.0	A sufficient level of danger
4	From 4.01 to 5.0	High level of danger

According to the research methodology to demonstrate the advantages of the proposed index over the existing one, condition (1) was used. The results of the experimental study of the region safety index, based on the theoretical sample, are shown in Table 7, where the primary assessments x_i, transformed assessments x_{i_t}, and the indices KS_{pr}, KS_{ex} are provided.

Table 7 – **Comparative analysis of the proposed (KS_{pr}) and existing (KS_{ex}) safety indices for regions constructed based on a theoretical sample of assessments**

№	x_1	x_2	x_3	x_4	x_{2_t}	x_{3_t}	KS_{ex}	KS_{pr}
1	1	1	1	1	1	1	0.2	1
2	1	1	1	2	1	1	0.25	1.125
3	1	1	2	1	1	2	0.35	1.125
…	…	…	…	…	…	…	…	…
625	5	5	5	5	5	5	5	5.0
SUM	1875	1875	1875	1875	1875	1875	1125	1562.5
RMSE							0.922	0.729

The comparative analysis of the proposed and existing state safety indices, based on the criterion of root mean square deviation, indicates the advantage of the proposed approach. Specifically, the root mean square error for the proposed and existing approaches is 0.729 and 0.922, respectively. This hypothesis is also confirmed in the experimental sample, as shown in Table 8.

The root mean square error obtained from the experimental results for the proposed and existing indices is 0.494 and 0.625, respectively. Using the assessments from Table 4, we build a machine learning model to predict the region's safety level, as shown in Table 9.

Based on the results of the constructed machine learning models, Decision Tree, Gradient Boosting, and Linear Regression models exhibit a process of overfitting, as indicated by the determination coefficients on the training/testing samples (1.0/0.99; 1.0/0.99; 0.94/0.93, respectively). Overfitting characteristics are confirmed by the dispersion index values (0.004; 0.003; 0.015, respectively) and bias values (0.03; 0.019; 0.007, respectively).

Table 8 – **Comparative analysis of the proposed (KS_{pr}) and existing (KS_{ex}) safety indices for regions constructed based on an experimental sample of assessments**

№	x_1	x_2	x_3	x_4	x_{2_t}	x_{3_t}	KS_{ex}	KS_{pr}
1	4	5	4	4	1.168	1.162	1.334	1.858
2	1	3	3	1	1.084	1.108	0.219	1.030
3	1	7	5	1	1.252	1.216	0.249	1.065
…	…	…	…	…	…	…	…	…
605	1	15	14	1	1.589	1.702	0.349	1.168
SUM	1227	5633	4523	1227	816.7	816.78	412.2	843.34
RMSE							0.625	0.496

Table 9 – **Results of investigating the performance indicators of machine learning models**

Researched approach	Linear Regression	Decision Tree	Random Forest	Gradient Boosting
R2train/R2test	0.94/0.93	1.0/0.99	0.99/0.99	1.0/0.99
MAE	0.085	0.008	0.007	0.009
MAX	0.671	0.259	0.269	0.233
RMSE	0.124	0.03	0.029	0.028
Bias	0.015	0.004	0.003	0.003
Variance	0.007	0.03	0.014	0.019

The Random Forest model demonstrates optimal accuracy values. Therefore, we will create hyperparameters to improve it in two steps.

The first step involves using n_estimators with values from 10 to 100, max_depth from 1 to 20, min_samples_split from 2 to 10, min_samples_leaf from 1 to 5, and max_features with 'auto', 'sqrt', 'log2'. Additionally, we set the number of iterations to 30 and the number of cross-validation folds to 5. In the second step, we add 'criterion' to the previous list with parameters 'poisson', 'squared_error', 'absolute_error', 'friedman_mse', 'bootstrap', 'oob_score' with parameters True, and the random number generation seed, as shown in Table 9.

Table 10 – **Comparative analysis of the Random Forest model based on region safety index evaluations, without hyperparameter tuning, and with hyperparameters**

Researched approach	Random Forest without hyperparameter	Random Forest ([('max_depth', 13), ('max_features', 'sqrt'), ('min_samples_leaf', 1), ('min_samples_split', 2), ('n_estimators', 79)])	Random Forest ([('bootstrap', True), ('criterion', 'squared_error'), ('max_depth', 13), ('max_features', 'auto'), ('min_samples_leaf', 1), ('min_samples_split', 2), ('n_estimators', 10), ('oob_score', True), ('random_state', 42)])
R2train/R2test	0.99/0.99	0.99/0.99	0.99/0.99
MAE	0.007	0.005	0.0075
MAX	0.269	0.083	0.303
RMSE	0.029	0.0139	0.0284
Bias	0.003	0.0005	0.001
Variance	0.014	-0.005	0.007

As seen from Table 6, Random Forest models, with different settings and without, achieve a compromise with a determination coefficient on the training/testing samples of 0.99/0.99. The values of dispersion and bias significantly decrease when using hyperparameters ([('max_depth', 13), ('max_features', 'sqrt'), ('min_samples_leaf', 1), ('min_samples_split', 2), ('n_estimators', 79)]) and are 0.0005 and -0.005, respectively. A negative value of dispersion indicates a slight probability of overfitting. To avoid this process, the number of hyperparameters has been increased following the research methodology.

The obtained determination coefficient values remained similar to the previous results, but the values of dispersion and bias increased, indicating signs of overfitting. Additionally, the values of MAE, MAX, RMSE increased in the model. Therefore, for predicting the region's safety index, it is recommended to use the Random Forest model ([('max_depth', 13), ('max_features', 'sqrt'), ('min_samples_leaf', 1), ('min_samples_split', 2), ('n_estimators', 79)]). This model is characterized by minimal overfitting probability in the future and has the following optimal quality indicators: MAE=0.005, MAX=0.083, RMSE=0.0139. The quality of the selected model is also confirmed by the learning curves, as shown in Fig. 1.

The learning curves of the Random Forest model ([('max_depth', 13), ('max_features', 'sqrt'), ('min_samples_leaf', 1), ('min_samples_split', 2), ('n_estimators', 79)]) confirm the sufficiency of the dataset for model construction and demonstrate the quality of determination coefficients for the training/testing samples. As shown in the graph, a sample size of 250 units and above is sufficient for conducting the research. The values of the determination coefficients stabilize and remain unchanged at 0.99.

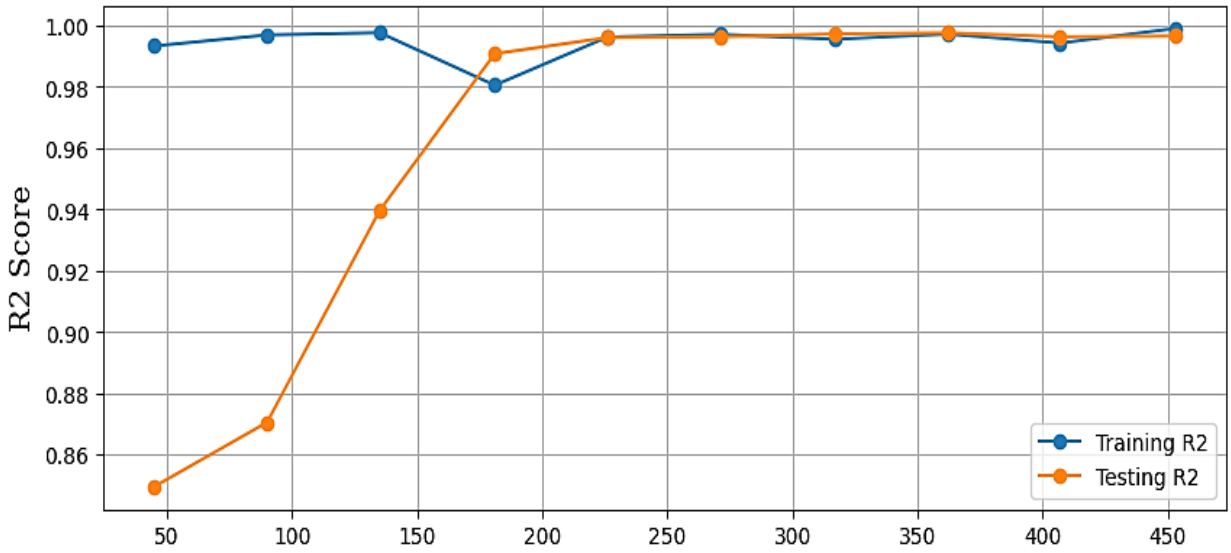

Fig. 1. Learning curves of the Random Forest model with hyperparameters set to [('max_depth', 13), ('max_features', 'sqrt'), ('min_samples_leaf', 1), ('min_samples_split', 2), ('n_estimators', 79)]

Let's consider a practical example of using the safety level prediction model. If we input 5, 1.25, 3.4, 4 into the constructed Random Forest machine learning model, we get a safety index level of 2.73. The obtained safety index value for the region indicates a medium level of danger.

The proposed index is characterized by the use of four variables: type of unmanned aerial vehicle or missile, the quantity of launched and hit objects, and the method of object launch. As seen in existing works [26, 27], models also consider time, object movements, additional coefficients to enhance the interrelation level. Additionally, it is worth considering meteorological conditions. From the perspective of mathematical operations, a linear model is proposed. If non-linear operations, such as squaring all variables and finding the overall sum, are added to the linear model, a more accurate model is obtained, with a mean squared error of 0.716.

However, incorporating these decisions will form a new approach to security prediction, so the proposed model has the mentioned limitations.

Conclusions

1. The task of developing a state security index is addressed by utilizing a linear model with combined variables, which, unlike existing models, takes into account the principles of variable interdependence, linear scaling, and exhaustive consideration of all combinations of assessments.

2. The task of developing a technology for predicting the security level of a region is solved by employing machine learning models, whose input assessments are determined using the state security index. The proposed approach has an advantage over existing ones in terms of mean squared error, which in the theoretical sample is 0.729; 0.922, respectively.

3. Experimental verification confirmed the hypotheses put forward, where in the experimental sample, the proposed approach also outperforms in terms of mean squared deviation: 0.496; 0.625, respectively.

The task of predicting the security of the region is addressed by using a Random Forest model with tuned hyperparameters. The model's adequacy is confirmed by minimal values of bias and variance: 0.0005; -0.005, respectively, a balance of determination coefficients on training and test samples: 0.99; 0.99, and learning curves.

Additionally, the proposed model demonstrates optimal quality indicators: MAE; MAX; RMSE 0.005; 0.083; 0.0139, respectively.

References

1. (2018), *About the national security of Ukraine*, the law of Ukraine, Verkhovna Rada information, 21.06.2018, No. 2469-VII, available at: https://zakon.rada.gov.ua/laws/show/2469-19#Text
2. Wamba, S.F., Bawack, R.E. and Carillo, K.D.A. (2019), "The State of Artificial Intelligence Research in the Context of National Security: Bibliometric Analysis and Research Agenda", *Lecture Notes in Computer Science*, 11701 LNCS, pp. 255–266, doi: https://doi.org/10.1007/978-3-030-29374-1_21
3. Francisco, M. (2023), "Artificial intelligence for environmental security: national, international, human and ecological perspectives", *Current Opinion in Environmental Sustainability*, 61, doi: https://doi.org/10.1016/j.cosust.2022.101250
4. Montasari, R. (2023), "Internet of Things and Artificial Intelligence in National Security: Applications and Issues", *Advances in Information Security*, vol. 101, pp. 27–56, doi: https://doi.org/10.1007/978-3-031-21920-7_3
5. Kuchuk, N., Kovalenko, A., Ruban, I., Shyshatskyi, A., Zakovorotnyi, O. and Sheviakov, I. (2023), "Traffic Modeling for the Industrial Internet of NanoThings", *2023 IEEE 4th KhPI Week on Advanced Technology*, KhPI Week 2023 – Conference Proceedings, 194480, doi: http://dx.doi.org/10.1109/KhPIWeek61412.2023.10312856

6. De Ruvo, G. (2022), "Data mining, artificial intelligence and national security: The geopolitical use of American legal infrastructure as an obstacle for a global data governance", *Rivista Italiana di Informatica e Diritto*, 2022(1), pp. 113–124, doi: http://dx.doi.org/10.32091/RIID0056
7. Kovalenko, A. and Kuchuk, H. (2022), "Methods to Manage Data in Self-healing Systems", Studies in Systems, Decision and Control, vol. 425, pp. 113–171, doi: https://doi.org/10.1007/978-3-030-96546-4_3
8. Montasari, R. (2022), "Artificial Intelligence and National Security", *Artificial Intelligence and National Security*, 230 p, doi: https://doi.org/10.1007/978-3-031-06709-9
9. Kharazishvili, Y. and Kwilinski, A. (2022), "Methodology for determining the limit values of national security indicators using artificial intelligence methods", *Virtual Economics*, vol. 5(4), pp. 7–26, doi: https://doi.org/10.34021/ve.2022.05.04(1)
10. Dun B., Zakovorotnyi, O. and Kuchuk, N. (2023), "Generating currency exchange rate data based on Quant-Gan model", *Advanced Information Systems*, Vol. 7, no. 2, pp. 68–74, doi: http://dx.doi.org/10.20998/2522-9052.2023.2.10
11. Al-Suqri, M.N. and Gillani, M. (2022), "A Comparative Analysis of Information and Artificial Intelligence Toward National Security", *IEEE Access*, 10, pp. 64420–64434, doi: http://dx.doi.org/10.1109/ACCESS.2022.3183642
12. Dotsenko, N., Chumachenko, I., Galkin, A., Kuchuk, H. and Chumachenko, D. (2023), "Modeling the Transformation of Configuration Management Processes in a Multi-Project Environment", *Sustainability (Switzerland)*, Vol. 15(19), 14308, doi: https://doi.org/10.3390/su151914308
13. Sanclemente, G.L. (2022), "Reliability: understanding cognitive human bias in artificial intelligence for national security and intelligence analysis", *Security Journal*, 35(4), pp. 87–91, doi: http://dx.doi.org/10.1057/s41284-021-00321-2
14. Datsenko, S., and Kuchuk, H. (2023), "Biometric authentication utilizing convolutional neural networks", *Advanced Information Systems*, vol. 7, no. 2, pp. 67–73. Doi: https://doi.org/10.20998/2522-9052.2023.3.10
15. Park, W.Y., Kim, S.H., Vu, D.-S., Jung, H.S. and Jo, H. (2022), "A Security System for National Network", *Lecture Notes in Networks and Systems*, 508 LNNS, pp. 789–803, doi: https://doi.org/10.1007/978-3-031-10467-1_48
16. Yaloveha, V., Podorozhniak, A. and Kuchuk, H. (2022), "Convolutional neural network hyperparameter optimization applied to land cover classification", *Radioelectronic and Computer Systems*, No. 1(2022), pp. 115–128, doi: https://doi.org/10.32620/reks.2022.1.09
17. Amponsah, A.A., Adekoya, A.F. and Weyori, B.A. (2022), "Improving the Financial Security of National Health Insurance using Cloud-Based Blockchain Technology Application", *International Journal of Information Management Data Insights*, vol. 2(1), 100081, doi: https://doi.org/10.1016/j.jjimei.2022.100081
18. Kuchuk, N., Mozhaiev, O., Semenov, S., Haichenko, A., Kuchuk, H., Tiulieniev, S., Mozhaiev, M., Davydov, V., Brusakova, O. and Gnusov, Y. (2023), "Devising a method for balancing the load on a territorially distributed foggy environment", *Eastern-European Journal of Enterprise Technologies*, vol. 1(4 (121), pp. 48–55, doi: https://doi.org/10.15587/1729-4061.2023.274177
19. Petrovska, I. and Kuchuk, H. (2023), "Adaptive resource allocation method for data processing and security in cloud environment", *Advanced Information Systems*, vol. *7*(3), pp. 67–73, doi: https://doi.org/10.20998/2522-9052.2023.3.10
20. Hashimov, E.G. and Khudeynatov, E.K. (2023), "The effectiveness of air defense system", *Advanced trends in the development of information and communication technologies and management tools*, 13 NTC, Baku, Kharkiv, Zhylina, vol. 1, pp. 17–18, doi: https://doi.org/10.32620/ICT.23.t1
21. Vavrin M., Zatonatska T. and Poltoratska A. (2023), "Clusterization of Ukraine regions according to the integrated index of ecological and economic security in the destructive phenomena conditions", *IOP Conference Series: Earth and Environmental Science*, 1150, no. 012019, pp. 1–10, available at: https://iopscience.iop.org/article/10.1088/1755-1315/1150/1/012019/pdf
22. Onyshchenko, S., Yanko, A., Hlushko, A. and Sivitska, S. (2022), "Increasing Information Protection in the Information Security Management System of the Enterprise", *Lecture Notes in Civil Engineering*, LNCE, vol 181, Springer, Cham., pp. 725–738, doi: https://doi.org/10.1007/978-3-030-85043-2_67
23. Onyshchenko, S., Shchurov, I., Cherviak, A. and Kivshyk, O. (2023), "Methodical approach to assessing financial and credit institutions' economic security level", *Financial and credit activity problems of theory and practice*, vol. 2, no. 49, pp. 65–78, doi: https://doi.org/10.55643/fcaptp.2.49.2023.4037
24. Ontalba, M.Á., Corbacho, J.Á., Baeza, A., Vasco, J., Caballero, J.M., Valencia, D. and Baeza, J.A. (2022), "Radiological Alert Network of Extremadura (RAREx) at 2021:30 years of development and current performance of on-real time monitoring", *Nuclear Engineering and Technology*, doi: https://doi.org/10.1016/j.net.2021.08.007
25. Zhu, W., Rodrigues, J.J.P.C., Niu, J., Zhou, Q., Li, Y., Xu, M. and Huang, B. (2019), "Detecting air-gapped attacks using machine learning", *Cognitive Systems Research*, vol. 57, pp. 92–100, doi: https://doi.org/10.1016/j.cogsys.2018.10.018
26. Van Dijcke, D., Wright, A. L. and Polyak, M. (2023), "Public response to government alerts saves lives during Russian invasion of Ukraine", *Proceedings of the National Academy of Sciences*, vol. 120, no. 18, doi: https://doi.org/10.1073/pnas.2220160120
27. Michalski, D. and Adam, R. (2020), "Counting the Uncountable", *Safety & Defense*, 2020, vol. 6, no. 2v pp. 100–112, doi: https://doi.org/10.37105/sd.91
28. Laktionov, A. (2021), "Improving the methods for determining the index of quality of subsystem element interaction", *Eastern-European Journal of Enterprise Technologies*, vol. 6(3 (114), pp. 72–82, doi: https://doi.org/10.15587/1729-4061.2021.244929
29. Borowska-Stefańska, M., Goniewicz, K., Grama , V., Hornak , M., Masierek, E., Morar , C., Penzes, J., Rochovska, A. and Wiśniewski, S. (2023), "Evaluating Approaches to Wartime Mass Evacuation Management in Eastern NATO Territories: A Literature Review", *Safety & Defense*, vol. 9(1), pp. 1–13, doi: https://doi.org/10.37105/sd.197

30. (2023), *Massive Missile Attacks on Ukraine*, available at: URL: https://www.kaggle.com/datasets/piterfm/massive-missile-attacks-on-ukraine

31. Campbell, A. (2020), *Python Guide: Clear Introduction to Python Programming and Machine Learning*, Independently Publ., 278 p., available at: https://www.amazon.com/Python-Guide-Introduction-Programming-Learning/dp/B0B7F4K4NK

Надійшла (received) 15.11.2023
Прийнята до друку (accepted for publication) 13.02.2023

ВІДОМОСТІ ПРО АВТОРІВ/ ABOUT THE AUTHORS

Шефер Олександр Віталійович – доктор технічних наук, професор, завідувач кафедри автоматики, електроніки та телекомунікацій, Національний університет "Полтавська політехніка імені Юрія Кондратюка", Полтава, Україна;
Oleksandr Shefer – Doctor of Technical Sciences, Professor, Head of the Department of Automation, Electronics and Telecommunications, National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine;
e-mail: itm.ovshefer@nupp.edu.ua; ORCID ID: https://orcid.org/0000-0002-3415-349X;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57210203269.

Лактіонов Олександр Ігорович – кандидат технічних наук, доцент кафедри автоматики, електроніки та телекомунікацій, Національний університет "Полтавська політехніка імені Юрія Кондратюка", Полтава, Україна;
Oleksandr Laktionov – Candidate of Technical Sciences, Associate Professor of the Department of Automation, Electronics and Telecommunications, National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine;
e-mail: itm.olaktionov@nupp.edu.ua; ORCID ID: https://orcid.org/0000-0002-5230-524X;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=58632082300.

Пенц Володимир Федорович – кандидат технічних наук, доцент, директор Навчально-наукового інституту інформаційних технологій та робототехніки, Національний університет "Полтавська політехніка імені Юрія Кондратюка", Полтава, Україна;
Volodymyr Pents – Candidate of Technical Sciences, Associate Professor, Director of the Educational and Research Institute of Information Technologies and Robotics, National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine;
e-mail: pents.olaktionov@nupp.edu.ua; ORCID ID: https://orcid.org/0000-0001-9580-1457;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57195421893.

Глушко Аліна Дмитрівна – кандидат економічних наук, доцент, доцент кафедри фінансів, банківського бізнесу та оподаткування, Національний університет "Полтавська політехніка імені Юрія Кондратюка", Полтава, Україна;
Alina Hlushko – Candidate of Economic Sciences, Associate Professor, Associate Professor of the Department of Finance, Banking and Taxation, National University "Yuri Kondratyuk Poltava Polytechnic", Poltava, Ukraine;
e-mail: glushk.alina@gmail.com; ORCID ID: https://orcid.org/0000-0002-4086-1513;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57202627340.

Кучук Ніна Георгіївна – доктор технічних наук, професор, професор кафедри обчислювальної техніки та програмування, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Nina Kuchuk – Doctor of Technical Sciences, Professor, Professor of Computer Engineering and Programming Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: nina_kuchuk@ukr.net; ORCID ID: http://orcid.org/0000-0002-0784-1465;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57196006131.

Практичні засади інтеграції штучного інтелекту в технологію прогнозування безпеки регіону

О. В. Шефер, О. І. Лактіонов, В. Ф. Пенц, А. Д. Глушко, Н. Г. Кучук

Анотація. Мета. Підвищення ефективності діагностики на предмет визначення рівня безпеки повітряної атаки за рахунок використання практичних засад інтеграції штучного інтелекту. **Методика.** Досліджено моделі та технології на предмет діагностики безпеки регіону (територіальної громади). Процес побудови моделі штучного інтелекту потребує диференціювання об'єктів на рівні для накопичення оцінок-характеристик літальних апаратів. Основою практичних засад інтеграції штучного інтелекту у технологію прогнозування є індекс безпеки регіону, котрий використовується для побудови моделей машинного навчання. Оптимальна модель машинного навчання запропонованого підходу обирається зі списку кількох моделей. **Результати.** Розроблено технологію прогнозування рівня безпеки регіону на основі індексу безпеки. У якості оптимальної моделі рекомендовано використовувати модель Random Forest ([('max_depth', 13), ('max_features', 'sqrt'), ('min_samples_leaf', 1), ('min_samples_split', 2), ('n_estimators', 79)]), що демонструє найефективніші показники якості MAE; MAX; RMSE 0,005; 0,083; 0,0139 відповідно. **Наукова новизна.** Запропонований підхід базується на основі лінійної моделі індексу безпеки регіону, що на відміну від існуючих враховує взаємодію факторів. Це дозволяє отримати переваги запропонованого методу над існуючими підходами за ознакою середньоквадратичного відхилення 0,496; 0,625 відповідно. У свою чергу, це впливає на якість моделей машинного навчання. **Практична значимість.** Запропоновані рішення є корисними для діагностики рівня безпеки регіону України, зокрема повітряних атак.

Ключові слова: прогнозування; лінійне рівняння; подвійна взаємодія; лінійне масштабування; індекс безпеки.