http://doi.org/10.35784/iapgos.8122 *received: 21.06.2025 | revised: 18.03.2026 | accepted: 16.04.2026 | available online: 30.06.2026*

MULTICRITERIA OPTIMISATION OF INFORMATION PROTECTION SYSTEM CONFIGURATION BASED ON THE NSGA-II ALGORITHM

Valeriy Lakhno[1], Myroslav Lakhno[1], Alona Desiatko[2], Bohdan Bebeshko[3]
[1]National University of Life and Environmental Sciences of Ukraine, Department of Computer Systems, Networks and Cyber Security, Kyiv, Ukraine, [2]State University of Trade and Economics, Department of Software Engineering and Cybersecurity, Kyiv, Ukraine, [3]Borys Grinchenko Kyiv Metropolitan University, Department of Information and Cyber Security named after Professor Volodymyr Buriachok, Kyiv, Ukraine

Abstract. *The article addresses the problem of multi-criteria optimisation of configuration parameters for an information protection system (IPS) within an enterprise or company. The problem lies in the difficulty of allocating a company's limited resources among the various components of the information security system (ISS) when there are conflicting requirements regarding security and performance. To address this challenge, it is proposed to integrate an analytical risk assessment model with the NSGA-II evolutionary algorithm. This results in the formation of a 3D Pareto front, which will enable the decision-maker to select a security configuration based on a visual analysis of five dimensions: reliability, performance, scalability, cost and compliance. This will eliminate the subjectivity inherent in methods that rely on a priori weighting coefficients. During the computational experiments, the influence of algorithm parameters on the formation of the solution set was examined, and Pareto fronts were visualised using the Plotly library. The trade-offs between the considered criteria were analysed. The results obtained confirmed the effectiveness of the proposed approach for selecting the optimal configuration of the protection system.*

Keywords: NSGA-II, Pareto-optimality, evolutionary algorithms, cybersecurity

WIELOKRYTERIALNA OPTYMALIZACJA KONFIGURACJI SYSTEMU OCHRONY INFORMACJI W OPARCIU O ALGORYTM NSGA-II

Streszczenie. *Artykuł porusza problem wielokryterialnej optymalizacji parametrów konfiguracyjnych systemu ochrony informacji (IPS) w przedsiębiorstwie lub firmie. Problem polega na trudnościach związanych z alokacją ograniczonych zasobów firmy pomiędzy różne elementy systemu bezpieczeństwa informacji (ISS) w sytuacji, gdy występują sprzeczne wymagania dotyczące bezpieczeństwa i wydajności. Aby sprostać temu wyzwaniu, proponuje się połączenie analitycznego modelu oceny ryzyka z algorytmem ewolucyjnym NSGA-II. Efektem tego jest utworzenie trójwymiarowej powierzchni Pareto, która umożliwi decydentowi wybór konfiguracji zabezpieczeń w oparciu o wizualną analizę pięciu wymiarów: niezawodności, wydajności, skalowalności, kosztu i zgodności z przepisami. Pozwoli to wyeliminować subiektywność charakterystyczną dla metod opartych na a priori ustalonych współczynnikach ważenia. W trakcie eksperymentów obliczeniowych zbadano wpływ parametrów algorytmu na tworzenie się zbioru rozwiązań, a fronty Pareto zwizualizowano przy użyciu biblioteki Plotly. Przeanalizowano kompromisy między rozpatrywanymi kryteriami. Uzyskane wyniki potwierdziły skuteczność proponowanego podejścia w wyborze optymalnej konfiguracji systemu zabezpieczeń.*

Słowa kluczowe: NSGA-II, optymalność Pareto, algorytmy ewolucyjne, cyberbezpieczeństwo

Introduction

Information protection systems (IPS) employed by companies and organisations to ensure cybersecurity (CS) are complex, multi-component, and multi-loop structures [20, 27]. Their effectiveness is determined by the interplay of multiple criteria [8, 9]. These criteria include, for instance, the balance between protection system reliability, performance, economic feasibility, scalability, degree of compliance with regulatory requirements, interoperability, fault tolerance, deployment time, and others [4, 5]. With the growing number of cyberattacks and the increasing complexity of their implementation scenarios, the optimisation of multi-loop protection systems remains a critical and timely challenge for organisations. Addressing this challenge requires a rigorous mathematical approach [2, 3], as the various criteria for evaluating the effectiveness of a protection system are often interdependent and mutually conflicting – such as cost versus effectiveness.

In this paper, we address the multi-criteria optimisation of IPS configuration parameters, enabling the determination of the Pareto-optimal set of solutions [1, 26]. The problem formalisation was based on defining a set of possible IPS configurations, represented as a parameter vector, and on five objective functions that characterise the key attributes of the IPS. The formal definition of a Pareto-optimal solution in this context relies on the principle that no single criterion can be improved without a simultaneous deterioration of at least one other criterion [6, 7]. To construct such a set of solutions, modern optimisation methods were employed. Specifically, the Non-dominated Sorting Genetic Algorithm II (NSGA-II) was utilised, which efficiently solves multi-criteria problems and ensures uniform coverage of the Pareto-optimal solution set. This approach enabled the consideration of trade-off solutions without the need to predefine weighting coefficients, making it suitable for complex, high-dimensional configuration problems in corporate anti-malware systems. The study focuses on the analytical description of the criteria and their interrelationships, as well as on the application of NSGA-II to efficiently identify balanced solutions.

1. Literature review

Information systems security assessment is a critical concern for any company or organisation. An effective protection system must consider numerous factors (criteria) that influence the company's life cycle. Several studies have proposed various approaches to quantitatively assessing cybersecurity (CS) levels and predicting potential threats. For instance, [25] explores methods for assessing CS under unknown threats by analysing attacker preferences. The authors treat zero-day attacks as long-term processes and apply game theory to forecast attacker behaviour, using Nash equilibrium to model potential attack scenarios and corresponding defensive strategies. A similar approach is adopted in [24], which proposes an attack-graph-based model that analyses the minimum number of vulnerabilities needed to compromise a system. However, this study does not account for defender preferences. Other research introduces broader metrics for evaluating CS. For example, in [23], the authors propose a targeted threat index that integrates factors related to social engineering and technical attacks. In [22], modelling techniques are applied to analyse attacker strategies, while in [21], time-delay neural networks are employed to predict attacker behaviour. It should be noted that game-theoretic models effectively describe the strategic interaction between an attacker and a defender at the micro-level. However, such models face computational complexity issues when scaled to the entire corporate security landscape. In contrast, the use of evolutionary algorithms, such as NSGA-II, has the potential to abstract away from the attacker's discrete moves and optimise the defence architecture at the macro level. Furthermore, NSGA-II can operate on system metrics under multi-criteria conditions.

Special attention is devoted to optimising the composition of information security systems. For instance, [20] presents a method for the operational optimisation of the composition of an information security protection subsystem that accounts for dynamic changes in operating conditions. The author proposes a model for this subsystem's operation that enables effective adaptation of its composition in response to evolving threats and requirements. In [19], an approach is considered for selecting security portfolios using a multi-task simulation-optimisation model, facilitating the effective balancing of various objectives, such as cost and level of protection, when forming security suites. However, the limited set of objective functions constrains the model's applicability. The authors of [17] conducted a review of optimisation methods for cyberinfrastructure security, analysing various models and approaches to improve information protection and proposing a systematisation. Nevertheless, specific objective functions are not defined in that study. In [16], the optimisation of security information and event management (SIEM) infrastructures, including event correlation and regression analysis, is investigated to achieve an optimal security posture. The study focuses on applying techniques to enhance threat detection and response; however, the composition of the SIEM tools themselves is not addressed. The work in [10, 11, 15] proposes a cost optimisation scheme based on vulnerability assessment to improve security efficiency. The authors explore how to reduce defence costs while enhancing effectiveness, but the set of cybersecurity criteria considered is rather limited. In [14], a comparative analysis and optimisation of patches within a cybersecurity framework are conducted, examining approaches for the efficient implementation of updates to protect against vulnerabilities. However, the problem of optimising the composition of the IPS itself remains unaddressed.

In [13], a review of the NSGA-II algorithm applied to multi-task combinatorial optimisation problems is presented, with its applications across various domains, including cybersecurity (CS), discussed. However, specific implementations within the CS domain are not examined. The work in [12] is essentially a survey of the use of the NSGA-II algorithm for multi-task optimisation. It discusses numerous applications of this method across different fields, including CS, and highlights its potential to solve complex optimisation problems. Nonetheless, a specific example of applying NSGA-II to the problem of selecting a company's IPS composition is not provided. As the analysis has shown, contemporary research in the CS domain offers a wide array of methods and metrics for analysing threats and vulnerabilities. However, unresolved challenges persist concerning the comprehensive assessment of system security in a multi-criteria environment. This paper proposes a multi-criteria optimisation approach to balance key information protection performance indicators, including reliability, performance, cost, scalability, and compliance.

2. Methods and models

The problem of multicriteria optimisation of IPS composition for corporate infrastructure is formalised as finding the optimal set of solutions in the space of alternative configurations, while accounting for conflicting requirements for cybersecurity (CS), performance, and economic efficiency. Let (X) denote the set of possible configurations of IPS, parameterised by $x \in X$, a vector of characteristics including technical, organisational and economic parameters. For each configuration defined criteria functions $f_i(x), i = 1,...,k,$ where k – the number of optimisation criteria.

Statement of the problem of multi-criteria optimisation of IPS for the enterprise (company). Denote: $x \in X$ – vector of IPS configuration parameters, where the set of possible solutions (In particular, in our study, this vector includes components such as hardware resource allocation, software complexity and licensing, administration time, network bandwidth, and the number of active compliance rules.)

$f(x) - \left(f_1(x), f_2(x), f_3(x), f_4(x), f_5(x)\right)$ – vector of target functions (criteria).

We accept the following target functions:

$f_1(x)$ – the indicator of protection reliability (the higher, the better);

$f_2(x)$ – the indicator of productivity (the higher, the better);

$f_3(x)$ – the cost of implementation (the lower, the better);

$f_4(x)$ – the indicator of scalability (the higher, the better);

$f_5(x)$ – the degree of compliance with regulatory requirements (the higher, the better).

The goal is to find a Pareto-optimal set of solutions that provides a trade-off between the criteria under consideration.

The formal definition of the Pareto-optimal solution can be written as follows $X^* = \left\{x^* \in X \mid \nexists x \in X : f_i(x) \geq f_i(x^*), \forall i = 1,...,k\right\}$ and for at least one i the inequality is strict. The constraints of the problem include regulatory requirements for CS, hardware and software infrastructure constraints, as well as budgetary and administrative limits, which are formalised by a system of constraints $g_i(x) \leq 0, j = 1,...,m.$ A solution x^* is called Pareto-optimal if there does not exist such $x \in X$, that $\forall i \quad f_i(x) \geq f_i(x^*)$, that and for at least one $i \quad f_i(x) > f_i(x^*)$. This means that one criterion cannot be improved without worsening at least one other criterion.

Each criterion describes a significant characteristic of the system. Thus, defence reliability $\left(f_1(x)\right)$ can be expressed as the probability of successfully preventing attacks, i.e.:

$$f_1(x) = 1 - P_{sa}(x) \tag{1}$$

where $P_{sa}(x)$ – the probability of a successful attack at a given IPS configuration, defined through a dependency of the form:

$$P_{sa}(x) = \frac{1}{1 + e^{\beta_1 \cdot R(x) - \beta_2 \cdot D(x)}} \tag{2}$$

where $R(x)$ – the level of threat detection (e.g., the percentage of detected attacks), $D(x)$ – the level of complexity of protection bypass (e.g., the number of different protection mechanisms used in the company), β_1, β_2 – model calibration parameters. The calibration parameters β_1 and β_2 are determined empirically based on a retrospective analysis of security incidents or expert assessments for a specific type of corporate network. The parameter β_1 reflects the system's sensitivity to the threat-detection rate, whilst β_2 characterising the non-linear decrease in the probability of a successful attack as defence-bypass mechanisms become more complex. For the purposes of this study, the values of these parameters have been selected to simulate a typical IT infrastructure of a medium-sized enterprise (SME). It is necessary to ensure that the values of the logistic function lie within the range of 0.05 to 0.95 for standard attack vectors.

Performance $\left(f_2(x)\right)$ is defined through the average response time of the system used in the IPS complex of the company. That is

$$f_2(x) = \frac{1}{T_r(x)} \tag{3}$$

where $T_r(x)=\frac{L_{rec}}{B(x)}+T_{pr}(x)$, L_{rec} average volume of input data, $B(x)$ system throughput, $T_{pr}(x)$ request processing time. The cost of IPS $(f_4(x))$ implementation generally includes hardware, software and support costs:

$$f_3(x)=C_{eq}(x)+C_{soft}(x)+C_{adm}(x) \quad (4)$$

where $C_{eq}(x)$ – the cost of hardware resources, $C_{soft}(x)$ – cost of licenses, $C_{adm}(x)$ – cost of administration and support.

Scalability $(f_4(x))$ determines the ability of an IPS to adapt to an increase in load, i.e.

$$f_4(x)=\frac{M_{valid}(x)}{M_{current}(x)} \quad (5)$$

where $M_{valid}(x)$ is the maximum number of users/data that the system can handle, $M_{current}(x)$ is the current number of users/data.

Compliance with regulatory requirements $(f_5(x))$ is represented through a binary penalty function, i.e.

$$f_5(x)=1\sum_{i=1}^{N} w_i\cdot\delta_i(x) \quad (6)$$

w_i weight of the penalty for non-compliance with the *i*-th normative requirement, $\delta_i(x)$ violation indicator (1 if it is violated, 0 if it is not).

It should be noted that the value M_{valid} assesses the company's IT department using a number of methods. For example, it is advisable to carry out regular load testing of the infrastructure and analyse the specifications provided by network and server equipment manufacturers, such as the maximum number of concurrent VPN sessions on the gateway. It is also possible to carry out a selection M_{valid} by extrapolating historical peak load data until network capacity bottlenecks arise.

To solve the multi-criteria optimisation problem, the scalarization method (convolution of criteria) and the Pareto-optimal ranking method were used.

For the first variant, i.e. the scalarization method, the convolution of criteria is used

$$\Phi(x)= \\ =\alpha_1\cdot f_1(x)+\alpha_2\cdot f_2(x)-\alpha_3\cdot f_3(x)+ \\ +\alpha_4\cdot f_4(x)+\alpha_5\cdot f_5(x) \quad (7)$$

where α_i are the weight coefficients determining the priority of criteria.

To construct the Pareto front, let us introduce a global constraint on the firm's resources:

$$\sum_{i=1}^{n} C_i(x)\le B_{\max} \quad (8)$$

where $C_i(x)$ – the cost of implementing the i-th security component; $B_{\max}$ – the company's maximum budget. Similar functional constraints link reliability and performance.

The introduction of strict functional constraints, such as a budget limit (B_{max}) and a maximum permissible response time (T_{max}), plays a key role in shaping the Pareto front. These prevent the so-called 'degeneration problem' in optimisation. In such a case, the algorithm could converge to trivial but physically unfeasible solutions, for example, a configuration with 100% reliability but infinite cost or zero throughput.

The classical approach assumes the solution of the problem, search $\max_{x\in X}\Phi(x)$ by methods of nonlinear programming. However, as modelling has shown, it is difficult to achieve an explicit Pareto front, see Fig. 1.

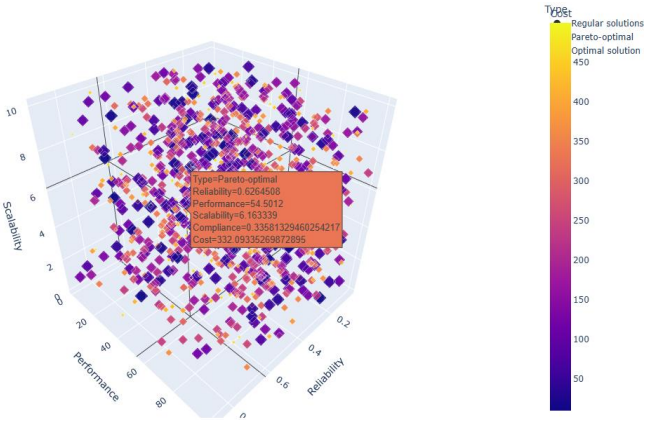


Fig. 1. Result of modelling based on the scalarization method (convolution of criteria

Therefore, the NSGA-II algorithm was employed in this study. To illustrate the proposed approach to multi-criteria optimisation of IPS configuration, the pseudocode below outlines the key stages of NSGA-II implementation, including defining objective functions, setting optimisation parameters, executing the Pareto-optimal search, and visualising the results. The pseudocode is intended to illustrate the algorithm's structure and main components, thereby facilitating a clearer understanding of the proposed solution.

Algorithm: Multi-Objective Optimisation using NSGA-II

Inputs:

- n_var: Number of decision variables (5).
  Vector X = [x_hw, x_sw, x_admin, x_bw, x_rules], where:
  x_hw: Hardware resources allocation
  x_sw: Software complexity and licensing
  x_admin: Administration and support hours
  x_bw: Network bandwidth capacity
  x_rules: Number of strict compliance rules activated
- n_obj: Number of objectives (5)
- n_constr: Number of constraints (2)
- xl, xu: Lower and upper bounds of decision variables
- pop_sizes: List of population sizes ([100, 500, 1000])
- mutation_probs: List of mutation probabilities ([0.1, 0.3, 0.5])
- termination_criterion: Number of generations (150)
- B_max: Maximum allowable budget constraint
- T_max: Maximum allowable response time constraint

Output:

- Pareto-optimal solutions and their visualisation

Begin

1. Define the optimisation problem:

a. Class SecurityOptimisationProblem:

i. Initialize with n_var, n_obj, n_constr, xl, xu.

ii. Define intermediate system dependencies mapping to Eq. (1)-(6):

- x_detect = f(x_sw, x_admin)
- x_complex = f(x_hw, x_sw)
- Capacity = f(x_hw, x_bw)

iii. Define _evaluate method:

// Objective 1: Reliability (Maximise -> minimise negative)

- P_attack = calculate_prob(x_detect, x_complex) // based on Eq. (2)
- f1 = -(1 - P_attack) // based on Eq. (1)

// Objective 2: Performance (Maximise -> minimise negative)

- T_response = calculate_response_time(Capacity) // based on Eq. (3)
- f2 = -(1 / T_response)
// Objective 3: Cost (Minimise)
- f3 = calculate_cost(x_hw, x_sw, x_admin) // based on Eq. (4)
// Objective 4: Scalability (Maximise -> minimise negative)
- f4 = -calculate_scalability(Capacity) // based on Eq. (5)
// Objective 5: Compliance (Maximise -> minimise negative)
- f5 = -calculate_compliance_penalty(x_rules) // based on Eq. (6)
// Define Problem Constraints (crucial for Pareto front formation)
- g1 = f3 - B_max // Constraint 1: Cost <= Budget
- g2 = T_response - T_max // Constraint 2: Response time <= Max allowed
- out["F"] = column_stack([f1, f2, f3, f4, f5])
- out["G"] = column_stack([g1, g2])

2. Initialise parameters:
a. pop_sizes = [100, 500, 1000]
b. mutation_probs = [0.1, 0.3, 0.5]
c. all_data = [] // To store valid results

3. For each combination of pop_size and mutation_prob:
a. Initialize NSGA-II:
i. Set population size, crossover (SBX), mutation (PM).
b. Run optimisation:
i. Minimise SecurityOptimisationProblem with NSGA-II.
c. Store results:
i. Append [Performance, Scalability, Reliability, Cost, Compliance, Parameters]
for non-dominated solutions to all_data.

4. Create DataFrame from all_data:
a. Columns: ["Performance", "Scalability", "Reliability", "Cost", "Compliance", "Parameters"]

5. Visualise Pareto-fronts using 3D scatter plot (Plotly):
a. Axes: X = Performance, Y = Scalability, Z = Reliability
b. Colour: Cost, Size: Compliance, Symbol: Parameters
c. Title: "Pareto-fronts (NSGA-II) with different hyperparameters"

6. Display the 3D plot.

End

Key features of the pseudocode presented above include a clear division into stages: 1) initialisation of the optimisation problem; 2) tuning of algorithm parameters; 3) execution of multi-criteria optimisation and visualisation of Pareto-fronts. The emphasis in the computational experiments is on using additional visual attributes (colour, marker size and shape) to represent the five criteria in three-dimensional space, thereby allowing us to visualise the trade-offs among reliability, performance, cost, scalability and compliance.

3. Model realization and computational experiments

The NSGA-II algorithm was employed as the optimisation method. The computational experiments were conducted in several stages, as outlined below.

Algorithm tuning was performed, during which various parameters of the NSGA-II algorithm - such as population size and mutation probability - were adjusted to examine their impact on the optimisation results. Subsequently, Pareto-optimal solutions were identified for each combination of algorithm parameters using NSGA-II. The resulting solutions were visualised in a 3D space, with additional attributes (colour, size, and marker shape) used to represent all five evaluation criteria.

Table 1 summarises the varying parameters used in the experiment, including algorithm parameters and IPS configuration options.

The algorithm parameters included population size and mutation probability. The population size ranged from 100 to 1000 individuals, enabling investigation of the impact of solution quantity on the diversity and quality of Pareto-optimal fronts. Mutation probabilities were set to 0.1, 0.3, and 0.5 to explore the trade-off between exploration of the search space and exploitation of already discovered solutions. The boundaries of the variables defining the search space were configured to encompass a broad range of possible IPS configurations.

Table 1. Varying parameters used in the experiment

Category	Parameter	Value options
Algorithm parameters	Population size (pop_size)	100, 500, 1000
	Mutation probability (mutation_prob)	0.1, 0.3, 0.5
IPS target functions	Reliability (f_1)	Maximization $f_1(x) = 1 - X[:,0]$
	Performance (f_2)	Maximization $f_2(x) = -X[:,1]$
	Cost (f_3)	Minimization $f_3(x) = X[:,2]$
	Scalability (f_4)	Maximization $f_4(x) = -X[:,3]$
	Regulatory compliance (f_5)	Maximization $f_5(x) = 1 - X[:,4]$
Variable limits	Lower limit	[0, 0, 0, 0, 0]
	Upper limit	[1, 100, 100, 10, 1]
Stopping criteria	Number of generations	150

The lower bounds for all variables were set to 0, while the upper bounds varied depending on the criterion. Specifically, the upper bound was set to 1 for reliability and regulatory compliance, to 100 for performance and cost, and to 10 for scalability. The stopping criterion for the algorithm was defined as a fixed number of generations, set to 150. The algorithm's termination criterion – 150 generations – is empirically justified by an analysis of the hypervolume metric. Test runs have shown that after 120–130 generations, the increase in hypervolume for populations of 500 and 1000 individuals is less than 0.5%. This result indicates the stabilisation of the set of non-dominant solutions and the algorithm's convergence.

The Plotly library was used in the computational experiments. In this case, to visualise the five criteria, the traditional 3D space can be extended by using additional visual attributes, such as the colour, size, and shape of markers, thereby emulating additional dimensions and enabling Pareto-front analysis for high-dimensional problems with more than three target functions. The basic idea is that the three key criteria (in our case, reliability, performance, and scalability of IPS) are displayed on the X, Y, Z axes, respectively. The remaining two criteria (cost and regulatory compliance) are visualised through additional marker attributes. So colour was used to represent cost, with a colour gradient reflecting the change in this parameter. The marker size represents the degree of regulatory compliance. Thus, each marker in the three-dimensional space conveys information about all five criteria, enabling the analysis of their interrelationships and trade-offs during the computational experiments. Additionally, the marker's shape can be used to further distinguish between different solution groups or IPS configurations. Specifically, round markers denote solutions that meet certain predefined conditions, while square markers indicate those that do not satisfy these conditions. This approach made it possible to identify key regions on the Pareto front where an optimal balance between criteria is achieved, or conversely, to detect regions where trade-offs between criteria are absent. Mathematically, such a visualisation can be described as follows. Let the five target functions considered in our

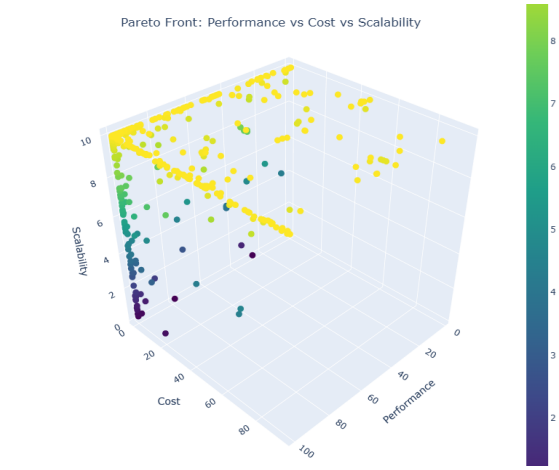
study be represented as $f_1(x), f_2(x), f_3(x), f_4(x), f_5(x)$. Then the three-dimensional space is given by the coordinates $f_1(x), f_2(x), f_3(x)$, and the additional attributes of the markers are defined as:

These represent the five objective functions considered in our study. Thus, the three-dimensional space is defined by coordinates, while additional marker attributes are specified as follows:

- marker colour $C(x) = f_4(x)$, where $C(x)$ – a function that maps cost to colour gradient;
- marker size $S(x) = f_5(x)$ where $S(x)$ – is a function that represents the degree of compliance with regulatory requirements in marker size;
- marker shape $F(x)$ where $F(x)$ – is a discrete function that defines the shape of the marker depending on additional conditions.

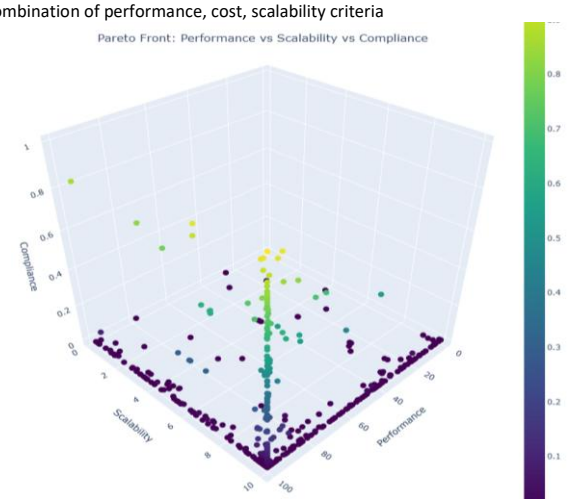
The simulation results are shown in Figures 2a–2d and Figure 3 for all 5 target functions.

a) combination of reliability, performance, cost criteria



b) combination of performance, cost, scalability criteria

c) combination of reliability, cost, compliance criteria



d) combination of performance, scalability, compliance criteria

Fig. 2. Combination of three target functions on separate graphs

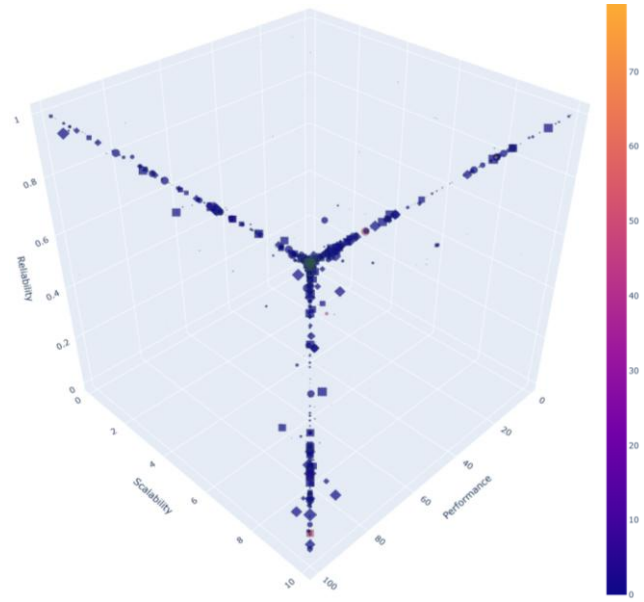


Fig. 3. Pareto-front display for 5 criteria in three-dimensional space

Thus, visualisation in Plotly, see Fig. 3 allowed us in computational experiments not only to display the Pareto front in 3D space, but also to emulate additional dimensions, making the analysis more informative.

Analysing the visualisation in Fig. 3, we note that diamond-shaped markers dominate this region. This corresponds to the largest population size and a high probability of mutation. Consequently, to find such extremely reliable but costly configurations, the algorithm will require a more extensive exploration of the search space. On the 3D plot, this group of solutions is visually highlighted by a cluster of squares. The dark colour of the markers in this zone indicates acceptable costs. However, the marker's minimal size suggests a shortfall in compliance with regulatory requirements.

From a practical perspective, a significant aspect of the study is the computational complexity of the proposed solution. Computational experiments were conducted on a standard workstation – an Intel Core i7 processor with 16 GB of RAM. The time taken to generate the Pareto front for a maximum population of 1,000 individuals over 150 generations was approximately 1.5–2 minutes. Such high execution speed confirms that this mathematical framework can be integrated into real-world decision-support software tools, enabling CISOs to evaluate ‘what-if’ scenarios in near real time.

4. Discussion of the results obtained and perspectives for follow-up research

The simulation results presented in Figs. 2 and 3 demonstrate the application of the multi-criteria optimisation method for tuning IPS parameters using the NSGA-II algorithm. The results are visualised as Pareto fronts, enabling a visual evaluation of the trade-offs among the considered criteria. Analysis of the results in Fig. 3 confirms that the NSGA-II algorithm effectively addresses the task of identifying Pareto-optimal solutions, providing uniform coverage of the set of possible IPS configurations. The visualisation in Fig. 3 is rendered in a three-dimensional space, where the key IPS criteria – reliability, performance, and scalability – are plotted along the axes. Cost and compliance are represented by the colour and size of the markers, respectively, enabling identification of regions where an optimal balance among the evaluated parameters is achieved.

Furthermore, different marker shapes (circles, squares, and rhombuses) are used to distinguish solutions obtained under varying algorithm parameter settings, specifically population size and mutation probability. The colour gradient, ranging from lighter to darker shades, encodes the cost criterion: darker markers indicate higher costs, enabling the identification of less cost-effective solutions. Marker size corresponds to the level of regulatory compliance, with larger markers indicating a higher level of compliance. This dual encoding of cost and compliance through colour and size provides a clear visual representation of the trade-offs between these criteria.

The use of distinct marker shapes enhances the interpretability of the results by grouping solutions based on the configurations of algorithm parameters. For instance, solutions generated with a population size of 100 and a mutation probability of 0.1 are represented by circles; those with a population size of 500 and a mutation probability of 0.3 are depicted as squares; and those with a population size of 1000 and a mutation probability of 0.5 are shown as rhombuses. This classification enables a comparative analysis of how different parameter settings influence the set of Pareto-optimal solutions.

The Pareto fronts are clearly distinguishable, with clusters of markers forming distinct regions in the three-dimensional space. These regions represent sets of solutions in which the improvement of one criterion inevitably leads to the deterioration of at least one other criterion, reflecting a fundamental property of Pareto optimality. The uniform distribution of markers across the fronts indicates that the NSGA-II algorithm effectively explores the solution space, yielding a diverse set of trade-off solutions.

It is important to note that the proposed approach eliminates the need to predefine weights for the criteria, which constitutes a significant advantage in environments where the prioritisation of criteria may be unclear or subject to change over time. Consequently, we believe that this approach is well-suited for practical application under real-world conditions in the formation of IPS architectures for companies, where system requirements may vary with external factors such as changes in regulatory frameworks or the emergence of new cyberattack types. The results of the study confirm that the application of multi-criteria optimisation techniques, such as NSGA-II, is an effective tool for configuring complex IPSs. Future research may explore the use of alternative optimisation algorithms, as well as the incorporation of additional criteria, such as resilience to novel threats or integration with existing cybersecurity systems.

The analysis of the Pareto front structure in Figures 2 and 3 enabled the identification of three distinct solution regions, each characterised by a specific distribution of the optimised parameter values. The first group of solutions is concentrated in the region with maximum values of the reliability function, accompanied by relatively low values of performance and scalability. This corresponds to IPS configurations in which the primary objective is to ensure system fault tolerance, typically achieved through strict protection policies. However, such configurations are associated with significant financial costs for IPS deployment. This region of the Pareto front reflects strategies typical of critical systems, where the presence of vulnerabilities or failures is deemed unacceptable.

The second group of solutions is represented by points exhibiting extremely high performance values, accompanied by minimised reliability and scalability indicators. This category of solutions may be applicable in scenarios where the system's cybersecurity is low criticality and performance is the primary concern.

The third region of the Pareto front corresponds to solutions with high scalability values but moderate or low levels of reliability and performance. These solutions are characterised by their ability to efficiently and dynamically adapt the IPS configuration, making them particularly relevant for distributed computing systems that require flexibility in responding to evolving cyber threats.

A detailed analysis of the Pareto front structure in Fig. 3 allowed us to identify regions containing solutions with optimised trade-offs among the considered criteria. From a multi-criteria decision-making perspective, the points located in the central part of the front are considered optimal, as they exhibit balanced values of IPS reliability, performance, and scalability. In contrast, the extreme points of the Pareto front correspond to configurations in which one criterion attains its maximum value at the expense of significant degradation in the other parameters, rendering them less favourable for practical implementation in protection systems.

A comparative analysis of the distribution of Pareto front points under different NSGA-II algorithm parameters, as shown in Figs. 2 and 3, demonstrates the influence of population size and mutation probability on the search process for optimal solutions. Variations in these evolutionary optimisation parameters lead to changes in the density distribution of points within the regions of compromise solutions. This observation highlights the need for further investigation into the impact of algorithmic hyperparameters on the quality of the resulting Pareto-optimal set. However, such an analysis falls outside the scope of the present study.

For the practical implementation of IPS, the decision-maker should select a single configuration from the resulting Pareto set. To this end, we propose applying the Analytic Hierarchy Process (AHP) or the TOPSIS method at the final stage. These methods will enable ranking the resulting non-dominated solutions according to the company’s current business priorities. A comparative analysis of the effectiveness of the proposed NSGA-II-based method against analogous algorithms, such as SPEA2, showed that NSGA-II provides a more uniform distribution of solutions across the front. Although it did require greater computational costs for the sorting operation.

5. Conclusions

In the course of this research, the problem of multi-criteria optimisation of IPS configuration parameters using the NSGA-II algorithm was formulated and solved. The obtained results enabled the identification of a set of Pareto-optimal solutions that offer a balanced compromise among reliability, performance, implementation cost, scalability, and compliance with regulatory requirements. Analysis of the resulting Pareto fronts demonstrated that the application of NSGA-II allows for efficient exploration of the solution space and the generation of alternative configurations aligned with varying strategic priorities of an organisation. The proposed approach eliminates the need to predefine weighting factors for the criteria, thereby enhancing its adaptability to evolving cybersecurity requirements. Visualisation of the results in three-dimensional space, supplemented with additional attributes, facilitated the interpretation of trade-offs between criteria and highlighted the most preferable configurations.

The scientific novelty of this research lies in the development of a comprehensive mathematical model that links the physical parameters of cyber defence components (bandwidth, information protection system update frequency) to macro-level performance

indicators. This relationship is modelled through a system of non-linear constraints. This approach has enabled us to avoid the problem from degenerating. The practical significance of the research lies in the creation of a ready-to-use analytical tool for Chief Information Security Officers (CISOs). This tool automates the configuration process for corporate security systems, providing CISOs with mathematically proven, balanced metrics across security, budget, and performance.

Future research is planned to expand the set of evaluation criteria by incorporating additional factors, such as resistance to emerging threat types and integration with existing cybersecurity systems. A comparative analysis of the effectiveness of various multi-criteria optimisation algorithms for solving the IPS configuration selection problem is also envisaged.

References

[1] Abraham, S., & Nair, S. (2018). Comparative analysis and patch optimization using the cyber security analytics framework. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, *15*(2), 161–180. https://doi.org/10.1177/1548512917705743

[2] Al-Jarrah, O., & Arafat, A. (2014). Network Intrusion Detection System using attack behavior classification. *2014 5th International Conference on Information and Communication Systems (ICICS)*, 1–6. https://doi.org/10.1109/IACS.2014.6841978

[3] Al-Kasasbeh, B. (2022). Model of the information security protection subsystem operation and method of optimization of its composition. *Egyptian Informatics Journal*, *23*(3), 511–516. https://doi.org/10.1016/j.eij.2022.05.003

[4] Boranbayev, A., Boranbayev, S., Nurusheva, A., & Yersakhanov, K. (2018). The Modern State and the Further Development Prospects of Information Security in the Republic of Kazakhstan. In S. Latifi (Ed.), *Information Technology – New Generations* (Vol. 738, pp. 33–38). Springer International Publishing. https://doi.org/10.1007/978-3-319-77028-4_6

[5] Carcary, M., Doherty, E., & Conway, G. (2019). A framework for managing cybersecurity effectiveness in the digital context. In T. Cruz, & P. Simoes (Eds.), *Proceedings of the 18th European Conference on Cyber Warfare and Security, ECCWS 2019* (Vol. 2019, pp. 78-86). (European Conference on Information Warfare and Security, Vol. 2019-July). Curran Associates Inc.

[6] Dreis, Y., Korchenko, O., Brzhevska, Z., Kriuchkova, L., & Nesterova, O. (2024). *Model to formation data base of internal parameters for assessing the status of the state secret protection*. *3654*, 277–289. https://ceur-ws.org/Vol-3654/paper23.pdf

[7] Dreis, Y., Korchenko, O., Sokolov, V., & Skladannyi, P. (2024). *Model to formation data base of secondary parameters for assessing status of the state secret protection*. *3800*, 1–11. https://ceur-ws.org/Vol-3800/paper1.pdf

[8] Ehis, A. T. (2023). Optimization of Security Information and Event Management (SIEM) Infrastructures, and Events Correlation/Regression Analysis for Optimal Cyber Security Posture. *Archives of Advanced Engineering Science*, 1–10. https://doi.org/10.47852/bonviewAAES32021068

[9] Ekelhart, A., Kiesling, E., Grill, B., Strauss, C., & Stummer, C. (2015). Integrating attacker behavior in IT security analysis: A discrete-event simulation approach. *Information Technology and Management*, *16*(3), 221–233. https://doi.org/10.1007/s10799-015-0232-6

[10] Enayaty-Ahangar, F., Albert, L. A., & DuBois, E. (2021). A survey of optimization models and methods for cyberinfrastructure security. *IISE Transactions*, *53*(2), 182–198. https://doi.org/10.1080/24725854.2020.1781306

[11] Hardy, S., Crete-Nishihata, M., Kleemola, K., Senft, A., Sonne, B., Wiseman, G., Gill, P., & Deibert, R. J. (2014). *Targeted Threat Index: Characterizing and quantifying politically-motivated targeted malware* (K. Fu, Ed.). USENIX Association.

[12] Jiang, Y., Jeusfeld, M. A., Ding, J., & Sandahl, E. (2023). Model-Based Cybersecurity Analysis: Extending Enterprise Modeling to Critical Infrastructure Cybersecurity. *Business & Information Systems Engineering*, *65*(6), 643–676. https://doi.org/10.1007/s12599-023-00811-0

[13] Kiesling, E., Ekelhart, A., Grill, B., Strauss, C., & Stummer, C. (2016). Selecting security control portfolios: A multi-objective simulation-optimization approach. *EURO Journal on Decision Processes*, *4*(1–2), 85–117. https://doi.org/10.1007/s40070-016-0055-7

[14] Ma, H., Zhang, Y., Sun, S., Liu, T., & Shan, Y. (2023). A comprehensive survey on NSGA-II for multi-objective optimization and applications. *Artificial Intelligence Review*, *56*(12), 15217–15270. https://doi.org/10.1007/s10462-023-10526-z

[15] Muminov, K., & Rustamova, M. (2024). Solving modern cybersecurity issues, a practical and experimental approach. *Engineering Problems and Innovations*, *2*(4), 18-26. https://doi.org/10.70037/epai.2.4.18-26

[16] Okimoto, T., Ikegai, N., Inoue, K., Okada, H., Ribeiro, T., & Maruyama, H. (2013). Cyber security problem based on Multi-Objective Distributed Constraint Optimization technique. *2013 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W)*, 1–7. https://doi.org/10.1109/DSNW.2013.6615540

[17] Palko, D., Babenko, T., Bigdan, A., Kiktev, N., Hutsol, T., Kuboń, M., Hnatiienko, H., Tabor, S., Gorbovy, O., & Borusiewicz, A. (2023). Cyber Security Risk Modeling in Distributed Information Systems. *Applied Sciences*, *13*(4), 2393. https://doi.org/10.3390/app13042393

[18] Park, J. Y., & Huh, E. N. (2020). A Cost-Optimization Scheme Using Security Vulnerability Measurement for Efficient Security Enhancement. *Journal of Information Processing Systems*, *16*(1), 61–82. https://doi.org/10.3745/JIPS.02.0128

[19] Serra, E., Jajodia, S., Pugliese, A., Rullo, A., & Subrahmanian, V. S. (2015). Pareto-Optimal Adversarial Defense of Enterprise Systems. *ACM Transactions on Information and System Security*, *17*(3), 1–39. https://doi.org/10.1145/2699907

[20] Shelupanov, A., Evsyutin, O., Konev, A., Kostyuchenko, E., Kruchinin, D., & Nikiforov, D. (2019). Information Security Methods—Modern Research Directions. *Symmetry*, *11*(2), 150. https://doi.org/10.3390/sym11020150

[21] Shukla, M., Sarmah, S. P., & Tiwari, M. K. (2023). A multi-objective framework for the identification and optimisation of factors affecting cybersecurity in the Industry 4.0 supply chain. *International Journal of Production Research*, *61*(15), 5266–5281. https://doi.org/10.1080/00207543.2022.2100840

[22] Shulha, O., Yanenkova, I., Kuzub, M., Muda, I., & Nazarenko, V. (2022). Banking Information Resource Cybersecurity System Modeling. *Journal of Open Innovation: Technology, Market, and Complexity*, *8*(2), 80. https://doi.org/10.3390/joitmc8020080

[23] Tagarev, N. (2019). A Critical Look at the Metrics for Measuring the Effectiveness of a Cybersecurity System. In Proceedings of International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE) (pp. 183-191).

[24] Verma, S., Pant, M., & Snasel, V. (2021). A Comprehensive Review on NSGA-II for Multi-Objective Combinatorial Optimization Problems. *IEEE Access*, *9*, 57757–57791. https://doi.org/10.1109/ACCESS.2021.3070634

[25] Wang, L., Jajodia, S., Singhal, A., Cheng, P., & Noel, S. (2014). k-Zero Day Safety: A Network Security Metric for Measuring the Risk of Unknown Vulnerabilities. *IEEE Transactions on Dependable and Secure Computing*, *11*(1), 30–44. https://doi.org/10.1109/TDSC.2013.24

[26] Yan, D. (2020). *A Systems Thinking for Cybersecurity Modeling* (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2001.05734

[27] Yin, L., Sun, Y., Wang, Z., Guo, Y., Li, F., & Fang, B. (2018). Security Measurement for Unknown Threats Based on Attack Preferences. *Security and Communication Networks*, *2018*, 1–13. https://doi.org/10.1155/2018/7412627

Dr. Valerii Lakhno
e-mail: lva964@nubip.edu.ua

Dr. Valerii Lakhno is a professor at the Department of Computer Systems, Networks and Cybersecurity at the National University of Life and Environmental Sciences of Ukraine, Ukraine. He holds a Ph.D. with a specialization in cybersecurity.
His areas of research include mathematical modelling, security of computer systems and networks, and intrusion recognition.

https://orcid.org/0000-0001-9695-4543

Eng. Myroslav Lakhno
e-mail: valss725@gmail.com

Myroslav Lakhno is a NET Full Stack Developer at e-Docs.UA. Education: National University of Life and Environmental Sciences of Ukraine, 2023. Research interests: IT, computer systems.

https://orcid.org/0000-0001-6979-6076

Dr. Alona Desiatko
e-mail: desyatko@gmil.com

Dr. Alona Desiatko is currently serving as Head of the Department of Software Engineering and Cyber Security, State University of Trade and Economics, Kyiv, Ukraine. She specializes in applying machine learning and cognitive modelling to solve complex problems in cybersecurity, cloud computing, and information systems. Her expertise also includes software architecture, as well as IT product and project management, with a focus on optimizing system performance and security.

https://orcid.org/0000-0002-2284-3418

Dr. Bohdan Bebeshko
e-mail: b.bebeshko@kubg.edu.ua

Dr. Bohdan Bebeshko is currently serving as associate professor at the Department of Information and Cyber Security named after Professor Volodymyr Buriachok, Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine. Bohdan's academic work investigates the integration of machine learning with cognitive modelling to enable personalization in digital learning systems. He specializes in user modelling and evidence-based decision-support approaches, particularly in the domains of information-risk management and adaptive content provision.

https://orcid.org/0000-0001-6599-0808