Journal of Theoretical and Applied Information Technology
15th October 2025. Vol.103. No.19

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

NUMERICAL METHODS FOR SOLVING NONLINEAR DIFFERENTIAL EQUATIONS IN INFORMATION NETWORK SECURITY PROBLEMS

MARYNA BELOVA[1], VOLODYMYR DENYSENKO[2], SVITLANA KARTASHOVA[3], VALERIJ KOTLYAR[4], STANISLAV MIKHAILENKO[5]

[1]Candidate of Physical and Mathematical Sciences, Associate Professor, Department of Digital Economy and System Analysis, Faculty of Information Technologies, State University of Trade and Economics, Kyiv, Ukraine

[2]Candidate of Physical and Mathematical Sciences, Associate Professor, Department of Digital Economy and System Analysis, Faculty of Information Technologies, State University of Trade and Economics, Kyiv, Ukraine

[3]Doctor of Biological Sciences, Candidate of Physical and Mathematical Sciences, Senior Research Officer, Chief Scientist, Department of European Integration and International Cooperation, The State Scientific and Technical Library of Ukraine, Kyiv, Ukraine

[4]Candidate of Physical and Mathematical Sciences, Associate Professor, Department of Digital Economy and System Analysis, Faculty of Information Technologies, State University of Trade and Economics, Kyiv, Ukraine

[5]Candidate of Physical and Mathematical Sciences, Associate Professor, Department of Digital Economy and System Analysis, Faculty of Information Technologies, State University of Trade and Economics, Kyiv, Ukraine

E-mail: [1]marynabelova1967@gmail.com, [2]volodya0232@ugmail.com, [3]kartashova_41@gmail.com, [4]arahna.val@gmail.com, [5]s2154_4788@gmail.com

ABSTRACT

The increasing complexity and dynamism of modern information networks makes the problem of their resistance to threats increasingly important. The use of differential equations, in particular, variants of epidemiological models, is one of the promising approaches to simulating the spread of harmful effects in such networks. This study proposes the use of numerical methods for solving nonlinear differential equations for modelling the dynamics of infection under different scenarios of cybersecurity threats. A scalable information network with a dynamic topology based on a stochastic block model is the basis of the experimental environment. The aim of the research is to determine the most effective numerical methods for modelling the spread of threats in information networks, taking into account accuracy, speed, and resistance to changes in parameters. Generalized models of the MeanField type were used to describe the spread of influence — both the basic one and its four nonlinear variations with exponential, logarithmic, quadratic, and power dependence, respectively. The models were solved using a wide range of numerical methods: classical adaptive methods (RK45, RK23, Radau, BDF, LSODA), as well as self-implemented schemes (Adams-Bashforth, Adams-Moulton). Large-scale experiments were conducted with varying network parameters (size, intensity of connections), initial conditions, model parameters, and integration step. The analysis was carried out using such metrics as accuracy (RMSE, Max Error), efficiency (execution time), and sensitivity to parameters. The obtained results gave grounds to determine the advantages of specific methods for different types of models and levels of system complexity. The prospects for further research include expanding models to multi-level networks, including stochastic components, and developing intelligent systems for choosing a numerical method in real time.

Keywords: *Nonlinear Differential Equations, Numerical Methods, Epidemiological Modelling, Information Security, Dynamic Network*.

1. INTRODUCTION

In the era of rapid digitalization, information networks (INs) are an important component of the infrastructure of almost all spheres of social life. They include public administration, financial systems, energy, medicine, etc. Their integration into key life processes leads to

increased requirements for the reliability, stability, and security of such systems. At the same time, cyber threats are complicating continuously: the number of attacks is increasing, the methods of unauthorized access are being improved, the use of automated botnets, social engineering, polymorphic malicious software (malware), etc. is being intensified [1], [2]. Traditional means of ensuring cybersecurity, based mainly on signature detection and reactive mechanisms, are becoming increasingly less effective in view of high dynamics and complexity of current attacks.

Therefore, there is a need for formalized approaches to modelling processes in cyberspace [3], which allow not only retrospective, but also predictive analysis. The use of differential equations (DE) [4], in particular nonlinear DE systems [5], is one of the most promising directions. This approach makes it possible to describe the dynamics of cyber threats, model the spread of malicious software, the interaction of attack and defence mechanisms, as well as the evolution of the state of the IM over time. The choice of numerical methods is of particular importance. They make it possible to calculate approximate solutions to the DE with high accuracy, adaptability to parametric changes, and taking into account complex input data.

So, the study of numerical methods for solving nonlinear DEs in the context of IM security analysis is relevant both from a scientific and applied perspectives. The novelty of the study is the constructed experimental environment for the systematic comparison of numerical methods in dynamic networks with various nonlinear threat propagation models that simulate the behaviour of computer viruses. The study takes into account not only the accuracy and solution time, but also the stability to parameter changes and scalability. The research hypothesis is that the most effective numerical methods can be identified among the available ones. They provide the best balance between accuracy, performance, and stability when modelling the propagation of harmful effects in dynamic networks. Therefore, the aim of this study is to compare and analyse the effectiveness of numerical methods for solving nonlinear DEs that describe the propagation of threats in IM. This makes it possible to identify the most accurate, fast, and stable approaches for practical application in modelling and ensuring cybersecurity. The aim was achieved through the fulfilment of the following research objectives:

1. Review modern approaches to mathematical modelling of IM security problems using DEs.
2. Identify the most common types of nonlinear models used in cyber threat analysis (e.g., epidemiological models of malware distribution).
3. Realize and test numerical methods for selected models and compare their efficiency and accuracy.
4. Build a simulation environment or a set of test scenarios in which models with numerical solutions can be used to assess the impact of attacks and the effectiveness of protective actions.

2. LITERATURE REVIEW

Many current studies focus on existing and development of new methods for numerical solution of DEs [6] of various types for solving a wide range of problems [7]. For example, the aim of the work [8] was to create a numerical method for solving first-order nodes (FNODE) by combining the trapezoidal method with a new semi-analytic technique.

The article [9] presents an improved algorithm of optimal homotopy analysis for working with nonlinear DEs. The study [10] also deals with the development of a new semi-analytic technique based on the homotopy analysis approach for solving linear or nonlinear DEs. The obtained results are compared with the methods of Adomy decomposition, homotopy perturbations, homotopy analysis, and optimized decomposition. The work [11] presents the method is that can be considered as an exact Bayesian inference by approximate likelihood. It is based on the discretization of a nonlinear differential operator to solve nonlinear partial differential equations.

In particular, much attention is focused on the study of DE solutions in cybersecurity problems. The use of probability distributions and DEs is quite popular for detecting the behaviour of malicious objects [12]. The research [13] proposes a dynamic model for detecting and predicting network intrusions based on fuzzy fractional ordinary Des. The method of decomposing the Fredholm linear integral equation into a piecewise Taylor series is used to obtain approximate solution expressions. In [14], the SEIARS model is proposed for modelling and analysing attacks in cyberspace. The dynamics of the model is governed by a set of DEs, which are usually solved by finite difference methods. The authors note limitations on the occupied memory space and the accumulation of approximation error at each step of finite difference methods.

The authors of [15] present a model that can simulate how malware spreads through the

network. But the model does not take into account all the possibilities for the network and the properties of the malware. The researchers continue to study its behaviour in the network and use graph theory and DE to reproduce the spread of the disease in computer networks.

In [16], a differential game model of network attack-defence is built based on the evolutionary analysis of network security states. Competitive analysis is performed based on the general attack and defence strategy, and the defence decision algorithm is developed based on the saddle point equilibrium strategy. In the article [17], the idea of applying the mathematical framework of differential transformations in the field of cybersecurity is developed. For this purpose, examples of using differential transformations to build models of cyberattack patterns for attack detection systems, mathematical models for assessing the security level of information and telecommunications systems are given.

The study [18] presents a method of time series analysis in the public security intelligence data analysis system, where a fractional differential operator is combined to build a mathematical model. Network intelligence is also analysed, a future case is predicted, and the predicted data is compared with the actual data for verification. The authors in [19] show that the model they proposed makes it possible to determine the transmission method used by the malware and the infection rate.

The aim of the paper [20] was to present a method for estimating an approximate solution of a nonlinear epidemiological model of computer viruses. The variational iteration method was applied for this purpose, and a comparison was made with the differential transformation method and the homotopy analysis transformation method. In the paper [21], the SAEIQRS (Susceptible – Antidotal – Exposed – Infected – Quarantine – Recovered – Susceptible) model of virus transmission in a computer network is proposed, where the differential transformation method is applied. The accuracy of the obtained results is confirmed by the RK4 method.

The research [22] deals with the approach to studying the global asymptotic stability of some epidemiological (based on DR) models that describe the spread of malware. The approach is based on the GAS theorem of time-continuous nonlinear cascade systems. The paper [23] investigates the SIR computer virus model as a nonlinear system of ordinary DEs using the homotopy analysis method (HAM).

The academic community currently shows significant interest in the application of numerical and semi-analytic methods for solving nonlinear dynamical processes for modelling complex dynamical processes in various fields. In particular, these methods are actively used in the field of cybersecurity. Researchers develop and improve approaches based on the homotopy analysis, differential transformations, Laplace decompositions, and fractional operators.

A number of studies present models of the spread of computer viruses and attacks using epidemiological analogies, graph theory, probabilistic analysis, and neural networks. Despite progress in this field, a number of aspects remain poorly studied.

The analysis of recent studies reveals significant progress in the development of numerical and semi-analytical methods for solving ordinary and partial differential equations (PDEs), which has enabled the modeling of complex dynamic processes in cybersecurity, including the spread of computer viruses, attack detection, and network security assessment. Approaches based on the homotopy method, differential transformations, variational iterations, fractional operators, and epidemiological analogies are widely used in the literature.

Despite the achieved results, there are still significant limitations in many studies:

- there is no consistent comparative analysis of numerical methods in terms of accuracy, speed, and stability in cyber threat modelling tasks;
- the topological complexity of real, especially large-scale, networks is often ignored or reduced to overly simplified models;
- a number of models neglect nonlinear dependencies in the dynamics of infection and recovery, which reduces their predictive ability; - there is no agreed methodology for assessing the effectiveness of methods in applied cyber defence.

These limitations create a need to develop an approach that combines realistic modelling of network structures, the use of nonlinear DRs, and modern numerical methods with a clear system for evaluating accuracy and computational efficiency.

Based on the identified gaps, this paper raises the following research questions:

Which numerical and semi-analytical methods provide the best balance between accuracy, speed, and stability in modelling the processes of cyberthreat propagation?

How does taking into account the topological complexity of the network affect the

accuracy and reliability of predicting the dynamics of attacks and virus infection?

Can the integration of realistic network models with nonlinear DRs improve the efficiency of cyberthreat detection and prediction compared to existing simplified approaches?

3. METHODS AND MODELS

3.1. Research Design

At each time step of the simulation, the network topology is updated with a given frequency to take into account the variability of connections. The network model is implemented in the form of a dynamic adjacency matrix *A(t)*, which is formed on the basis of a given probability matrix of connections for clusters. This enables reflecting both the logical structure of the network and its behaviour over time. Such a structure provides a high degree of realism in the simulation of the spread of harmful effects.

MeanField variants with nonlinear dependencies are used as a propagation model, as well as numerical methods for solving differential equations (RK45, Radau, BDF, etc.). The following metrics are calculated at each step of the experiment: RMSE, peak infection, total number of recoveries, and calculation time. A total of 120 experiments were performed for each method. The general research design is presented in Figure 1.

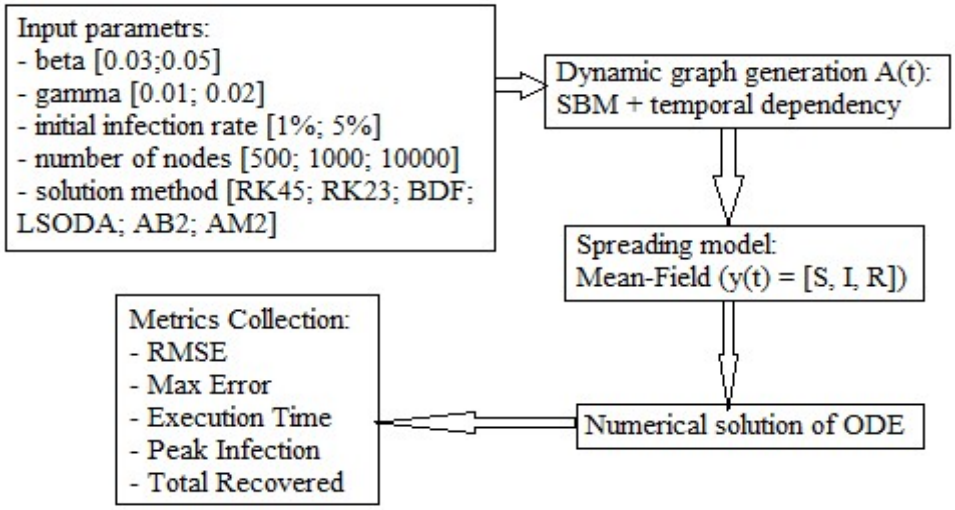

Figure 1. Research design
Source: created by the author

3.2. Sample

The experimental data set was generated by numerical simulations on simulated INs of different scales. Three network sizes were chosen: 500, 1,000, and 10,000 nodes. Simulations were performed with different initial conditions for each network: infection rates 1% and 5% and model parameters ($\beta \in \{0.03, 0.05\}$, $\gamma \in \{0.01, 0.02\}$). Each configuration was tested using several numerical solution methods to collect a representative sample for comparative analysis of the accuracy and efficiency of the methods under different conditions. This choice is determined by the aspiration to model a structured but flexible IN architecture that is close to real conditions.

3.3. Research Methods

The spread of infectious effects in an information security network was modelled by using the MeanField approach as a generalization of the SIR model [24], [25]. It describes the dynamics of the transition of individuals between three states: susceptible to infection (S), infected (I), and recovered (R).

$$\begin{aligned} \frac{dS}{dt} &= -\beta S(t) \cdot \left(A \cdot I(t)\right) \\ \frac{dI}{dt} &= \beta S(t) \cdot \left(A \cdot I(t)\right) - \gamma I(t) \\ \frac{dR}{dt} &= \gamma I(t)^{1.1} \end{aligned} \quad (1)$$

where β – infection transmission coefficient;

A – the matrix of connections between network nodes;

$I(t)$ – the vector of infected nodes at time t;

γ – recovery coefficient.

The MeanField model [26] describes the dynamics of the three groups (susceptible, infected, and recovered) as follows:

$$\begin{cases} \frac{dS}{dt} = -\beta SI \\ \frac{dI}{dt} = \beta SI - \gamma I \\ \frac{dR}{dt} = \gamma I \end{cases} \quad (2)$$

In addition to the basic version, the paper proposes five modifications of the MeanField model that take into account the nonlinear characteristics of the real infection or recovery process:

MeanField_1 Exponential infection:

$$\begin{cases} \frac{dS}{dt} = -\beta S e^{\alpha I} \\ \frac{dI}{dt} = \beta S e^{\alpha I} - \gamma I \\ \frac{dR}{dt} = \gamma I \end{cases} \quad (3)$$

This simulates a situation where α is the level of exponential susceptibility, increasing its value causing a sharper infection with increasing I. It simulates scenarios where automatic spread or reinfection leads to an explosive increase in infection.

MeanField_2 Logarithmic infection:

$$\begin{cases} \frac{dS}{dt} = -\beta S \ln(1 + \alpha I) \\ \frac{dI}{dt} = \beta S \ln(1 + \alpha I) - \gamma I \\ \frac{dR}{dt} = \gamma I \end{cases} \quad (4)$$

In this case, the infection grows more slowly with large I. It simulates the saturation effect, where new infections are reduced by antivirus protection, automatic node blocking.

MeanField_3 Quadratic recovery rate:

$$\begin{cases} \frac{dS}{dt} = -\beta SI \\ \frac{dI}{dt} = \beta SI - \gamma I^2 \\ \frac{dR}{dt} = \gamma I^2 \end{cases} \quad (5)$$

In this model, increasing the number of infected makes recovery more difficult. It reflects the overload of the recovery system. This is observed in DoS/DDoS attacks.

MeanField_4_1 and MeanField_4_2 Indicative infection:

$$\begin{cases} \frac{dS}{dt} = -\beta SI^k \\ \frac{dI}{dt} = \beta SI^k - \gamma I \\ \frac{dR}{dt} = \gamma I \end{cases} \quad (6)$$

In this model, the infection depends on the degree k, which provides flexible modelling of different types of spread: from gradual to explosive, including scattering or cluster propagation effects. For $k<1$, sublinear propagation (MeanField_4_1), for $k>1$ — very fast propagation (MeanField_4_2).

The paper compares the following methods for numerical solutions of DEs: Runge-Kutta, Radau, Backward Differentiation Formula, LSODA, Adams-Bashforth 2 and Adams-Moulton 2 methods.

1-2. Runge-Kutta (RK) methods [27] are a family of numerical methods for approximate solution of systems of ordinary differential equations. The RK45 and RK23 methods are special cases of the Runge-Kutta method, which use an adaptive time step to achieve the desired accuracy of the solution. In RK45, the step h is adjusted depending on the error estimate between the 4th and 5th order steps. For RK23, the 2nd and 3rd order estimates are used.

Mathematical formulation of the problem for solving the SIR equations (1):

$$y(t) = \begin{bmatrix} S(t) \\ I(t) \\ R(t) \end{bmatrix} \quad (7)$$

The system of equations looks like this:

$$\frac{dy}{dt} = \begin{bmatrix} \frac{dS}{dt} \\ \frac{dI}{dt} \\ \frac{dR}{dt} \end{bmatrix} = \begin{bmatrix} -\beta S(t) \cdot (A \cdot I(t)) \\ -\beta S(t) \cdot (A \cdot I(t)) - \gamma I(t) \\ \gamma I(t)^{1.1} \end{bmatrix} \quad (8)$$

The estimates k_1, k_2, k_3, k_4, k_5 are used for the RK45 method, which are calculated at each stage:

$$\begin{aligned} k_1 &= h \cdot f(t_n, y_n); \\ k_2 &= h \cdot f\left(t_n + \frac{h}{4}, y_n + \frac{k_1}{4}\right); \\ k_3 &= h \cdot f\left(t_n + \frac{h}{4}, y_n + \frac{k_2}{4}\right); \end{aligned} \quad (9)$$

$$k_4 = h \cdot f\left(t_n + \frac{h}{2}, y_n + \frac{k_2}{2}\right);$$
$$k_5 = h \cdot f(t_n + h, y_n - k_3 + 2k_4)$$

After these calculations, they are combined to obtain values for the next step:

$$y_{n+1} = y_n + \frac{1}{6} \cdot (k_1 + 4k_2 + k_3) \quad (10)$$

3. The Radau method [28] is an implicit method for solving stiff DEs. It uses a scheme where it is necessary to solve a system of equations to obtain the values at the next step. In general, for each step we can write:

$$y_{n+1} = y_n + h \sum_{i=1}^{r} a_i k_i, \quad (11)$$

where α_i – coefficients, k_i – derivatives calculated at each stage.

4. The BDF (Backward Differentiation Formula) method is an implicit method for solving hard conventional differential equations that uses difference schemes to calculate derivatives based on values at previous points. For an equation of the form:

$$\frac{dy}{dt} = f(t, y) \quad (12)$$

the BDF method can be presented as follows:

$$\frac{y_{n+1} - y_n}{h} = a_1 f(t_{n+1}, y_{n+1}) + a_2 f(t_n, y_n) \quad (13)$$

where α_1 and α_2 – coefficients for each stage.

The method is effective for systems where there are rapid changes in the values of some variables (e.g., infection rate) and slow changes in others (e.g., recovery).

5. LSODA (Livermore Solver for Ordinary Differential Equations with Automatic Method Switching) is an adaptive numerical method for solving ordinary DEs that automatically chooses between the RK method for non-stiff systems and the BDF method for stiff systems. This gives greater stability at large time steps.

6. Adams-Bashforth2 (AB2) [29] is an explicit method that uses the first two integration steps to estimate the next value of the solution. It has the following form:

$$y_{n+2} = y_{n+1} + \frac{h}{2}(3 f(t_{n+1}, y_{n+1}) - f(t_n, y_n)) \quad (14)$$

where y_{n+2} – the solution at the next step;

y_{n+1}, y_n – the values of the previous solutions;

$f(t, y)$ – the function describing the right-hand side of the equation.

The method is explicit, so it is easy to implement and has high speed, but it is not always stable at large h for rigid systems.

7. Adams-Moulton2 [29] is an implicit method that uses the values at the current and previous points to correct the estimate of the future value. It is a more accurate method compared to AB2, because it uses an additional value y_{n+1} for correction. It can be represented as follows:

$$y_{n+2} = y_{n+1} + \frac{h}{2}(f(t_{n+2}, y_{n+2}) + 3 f(t_{n+1}, y_{n+1})) \quad (15)$$

4. RESULTS

A multivariate analysis of the effectiveness of numerical methods for solving DEs for different variations of MeanField-type models was conducted in the course of the experimental study. The evaluation was carried out by accuracy (RMSE) and time efficiency (T). The average values of RMSE and execution time are given in Table 1. The accuracy of each method was calculated relative to the solution obtained by the RK45 method, as it is considered a reliable basic integrator with an adaptive step for conventional DE problems.

Table 1: Average values of RMSE and T for each method

Metric	RK45	RK23	BDF	RADAU	LSODA	AB2	AM2
RMSE	0.00E+00	3.43E-05	1.21E-05	4.18E-05	3.00E-05	1.19E-05	3.57E-05
Time, c	1.22E-03	1.52E-03	3.36E-03	4.64E-03	1.14E-03	4.55E-03	1.18E-02

Source: calculated by the author

The analysis of the average RMSE and T of seven numerical methods used to solve nonlinear models of threat propagation dynamics in IN found significant differences. The best accuracy is shown by AB2 (1.19×10^{-5}) and Radau (1.21×10^{-5}).

The RK23, LSODA, and AM2 methods have an average level of accuracy for RMSE in the

range of 3.0×10^{-5} – 3.6×10^{-5}. The BDF method in this case showed the highest error (4.18×10^{-5}). This may indicate its less effective adaptation to the specifics of the problem or sensitivity to parameters.

Regarding T, LSODA turned out to be the fastest (1.14×10^{-3} s). Implicit methods showed the highest time consumption: Radau (4.64×10^{-3} s), AB2 (4.55×10^{-3} s) and especially AM2 (1.18×10^{-2} s). This is quite logical, given the nature of the iterative correction procedure.

Tables 2 and 3 provide a more detailed analysis of the accuracy and T, respectively. The data are averaged for each method by model, number of network nodes, β and γ parameters, and initial infection percentage. The accuracy of each method was calculated relative to the solution obtained by the RK45 method.

Table 2: Average RMSE values of the studied methods for different groups of parameters

Model	RK45	RK23	BDF	RADAU	LSODA	AB2	AM2
MeanField_1	0.00E+00	2.21E-05	4.40E-05	7.84E-06	2.20E-05	7.97E-06	3.78E-05
MeanField_2	0.00E+00	3.25E-06	5.56E-06	3.11E-07	1.30E-06	2.82E-07	6.25E-06
MeanField_3	0.00E+00	7.44E-05	5.57E-05	2.35E-05	7.03E-05	2.45E-05	9.45E-05
MeanField_4_1	0.00E+00	1.20E-06	3.83E-06	2.17E-07	8.38E-07	5.45E-08	3.16E-06
MeanField_4_2	0.00E+00	7.06E-05	1.00E-04	2.84E-05	5.55E-05	2.68E-05	3.66E-05
Number of nodes	RK45	RK23	BDF	RADAU	LSODA	AB2	AM2
500	0.00E+00	3.43E-05	4.18E-05	1.21E-05	3.00E-05	1.19E-05	3.57E-05
1000	0.00E+00	3.43E-05	4.18E-05	1.21E-05	3.00E-05	1.19E-05	3.57E-05
10000	0.00E+00	3.43E-05	4.18E-05	1.21E-05	3.00E-05	1.19E-05	3.57E-05
β	RK45	RK23	BDF	RADAU	LSODA	AB2	AM2
0,03	0.00E+00	2.19E-05	2.42E-05	6.96E-06	1.89E-05	5.77E-06	2.92E-05
0,05	0.00E+00	4.67E-05	5.95E-05	1.71E-05	4.10E-05	1.81E-05	4.21E-05
γ	RK45	RK23	BDF	RADAU	LSODA	AB2	AM2
0,01	0.00E+00	3.72E-05	4.26E-05	1.04E-05	3.33E-05	1.03E-05	3.62E-05
0,02	0.00E+00	3.14E-05	4.10E-05	1.37E-05	2.66E-05	1.35E-05	3.51E-05
Infected	RK45	RK23	BDF	RADAU	LSODA	AB2	AM2
1%	0.00E+00	3.28E-05	3.44E-05	5.71E-06	2.08E-05	6.25E-06	3.66E-05
5%	0.00E+00	3.58E-05	4.93E-05	1.84E-05	3.92E-05	1.76E-05	3.47E-05

Source: calculated by the author

Radau and AB2, especially on MeanField_2 and MeanField_4_1 show the lowest error values. The largest errors are found in AM2, RK23 and BDF, with peaks on MeanField_3 and MeanField_4_2, which indicates their sensitivity to the nonlinearity of these models. The RMSE value practically does not change with increasing number of nodes. This indicates the stability of the methods to scaling within one model. With increasing β, an increase in the error is observed in all methods. This is explained by the strengthening of the nonlinear $S{\cdot}I$ interaction or other I functions that complicate the dynamics of the system.

With increasing γ, the error decreases slightly in most methods (especially in RK23, BDF, LSODA), which can be explained by faster stabilization of the system. For a larger value of the initial contamination (5%), the error increases in BDF, RK23, AM2, which indicates increased sensitivity to a sharp initial perturbation. Radau and AB2 remain stable.

Table 3: Average T values of the studied methods for different groups of parameters

Model	RK45	RK23	BDF	RADAU	LSODA	AB2	AM2
MeanField_1	1.15E-03	1.47E-03	4.94E-03	3.17E-03	1.07E-03	4.35E-03	1.20E-02
MeanField_2	1.43E-03	1.31E-03	3.93E-03	2.83E-03	1.08E-03	6.40E-03	1.24E-02
MeanField_3	1.10E-03	1.75E-03	4.11E-03	3.57E-03	1.17E-03	3.80E-03	1.14E-02
MeanField_4_1	1.08E-03	1.13E-03	3.64E-03	2.49E-03	9.00E-04	3.95E-03	9.55E-03
MeanField_4_2	1.33E-03	1.96E-03	6.58E-03	4.74E-03	1.48E-03	4.26E-03	1.35E-02
Number of nodes	RK45	RK23	BDF	RADAU	LSODA	AB2	AM2
500	1.29E-03	1.48E-03	4.45E-03	3.26E-03	1.10E-03	4.74E-03	1.21E-02
1000	1.16E-03	1.43E-03	4.80E-03	3.25E-03	1.17E-03	4.38E-03	1.14E-02
10000	1.22E-03	1.67E-03	4.67E-03	3.57E-03	1.15E-03	4.54E-03	1.18E-02
β	RK45	RK23	BDF	RADAU	LSODA	AB2	AM2
0,03	1.27E-03	1.55E-03	4.41E-03	3.16E-03	1.13E-03	4.61E-03	1.07E-02
0,05	1.16E-03	1.49E-03	4.87E-03	3.56E-03	1.15E-03	4.50E-03	1.29E-02
γ	RK45	RK23	BDF	RADAU	LSODA	AB2	AM2
0,01	1.23E-03	1.59E-03	4.38E-03	3.25E-03	1.10E-03	4.48E-03	1.12E-02
0,02	1.21E-03	1.46E-03	4.90E-03	3.47E-03	1.18E-03	4.63E-03	1.23E-02
Infected	RK45	RK23	BDF	RADAU	LSODA	AB2	AM2
1%	1.27E-03	1.64E-03	4.57E-03	3.38E-03	1.13E-03	4.56E-03	1.18E-02
5%	1.17E-03	1.41E-03	4.71E-03	3.34E-03	1.15E-03	4.55E-03	1.17E-02

Source: calculated by the author

Methods: LSODA and RK45 (≈1.1E-03...1.4E-03) have stable performance regardless of the model. The AM2 method demonstrates low speed (1.2E-02...1.35E-02) because of iterativeness and implicit nature. BDF has an average time that increases with model complexity (MeanField_4_2). The time increases by 15–20% when going from 500 to 10,000 nodes. This indicates a satisfactory scalability of the implementation due to the use of vectorized calculations.

With increasing β, an increase in time is observed for all methods, as more intense dynamics require more iterations for an accurate solution. Increasing γ almost does not change the execution time, but slightly affects AM2 and AB2. Changing the percentage of initial infection slightly affects the T of the methods. Figures 2-7 show the histograms of RMSE and peak error separately for each method throughout all experiments.

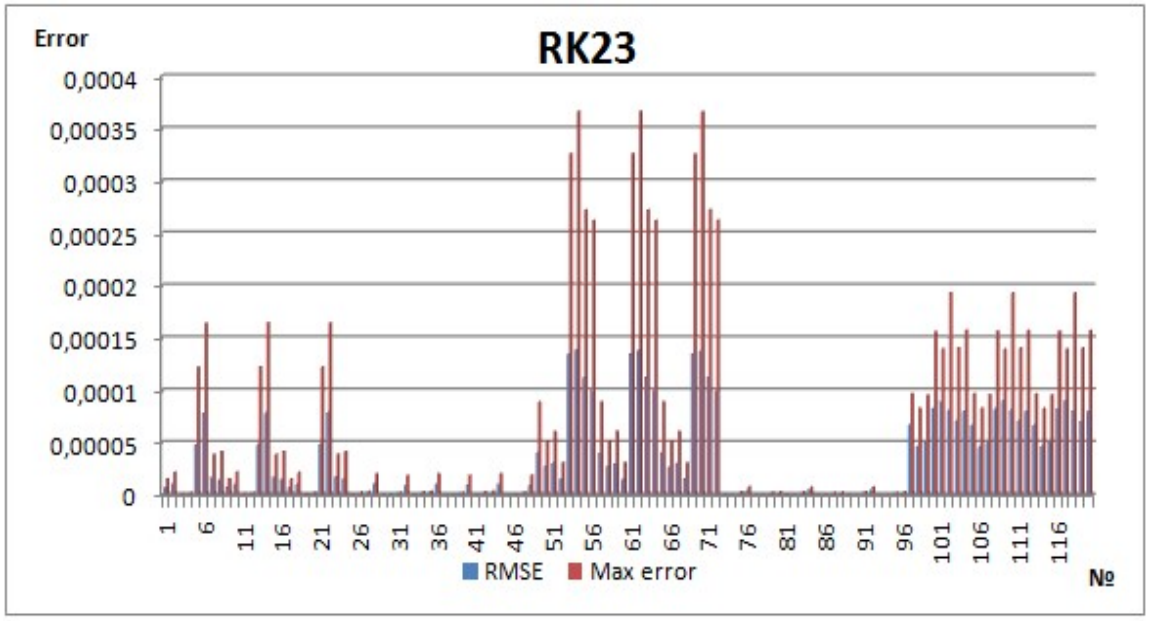

Figure 2: Histogram of RMSE and MaxError for RK23
Source: created by the author

The histogram (Figure 2) shows a stable RMSE value throughout the series of experiments. However, the MaxError values have sharp jumps in the experiments with the MeanField_3 and MeanField_4_2 models. With the Mean]Field_2 and MeanField_4_1 models, these metrics differ slightly from 0.

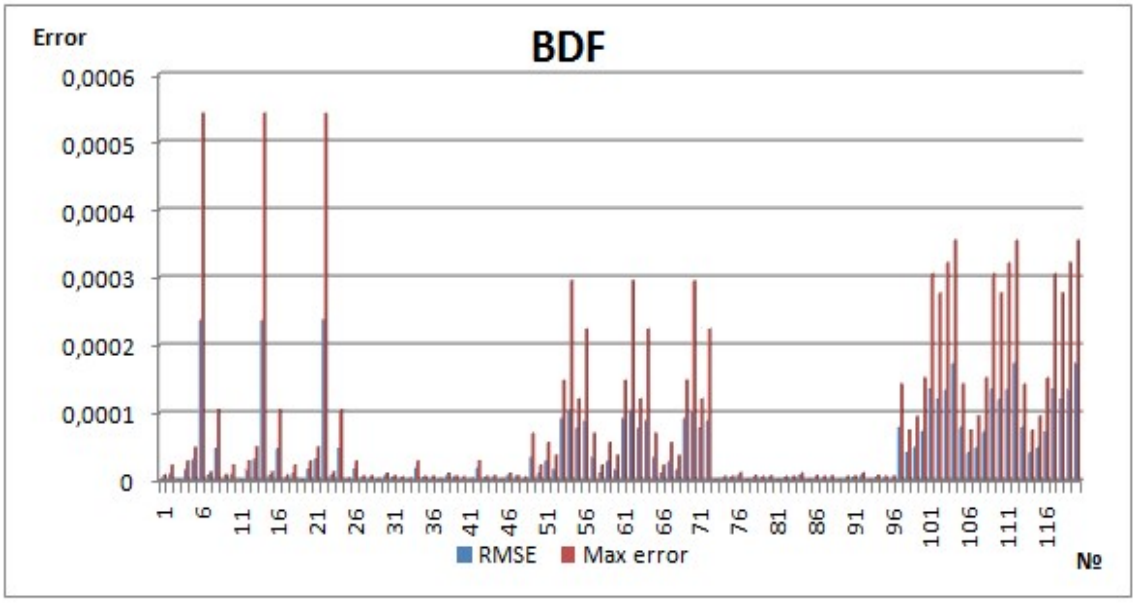

Figure 3: Histogram of RMSE and MaxError for BDF
Source: created by the author

Figure 3 shows that low values and a relatively stable change in RMSE are observed when applying the BDF method. High jumps in MaxError values are observed, especially at points 6, 14, and 22. This occurs when model 1 is applied and the parameters β=0.05; γ=0.01; the initial infection percentage is 5%, and the number of nodes is 500, 1000 and 10000, respectively.

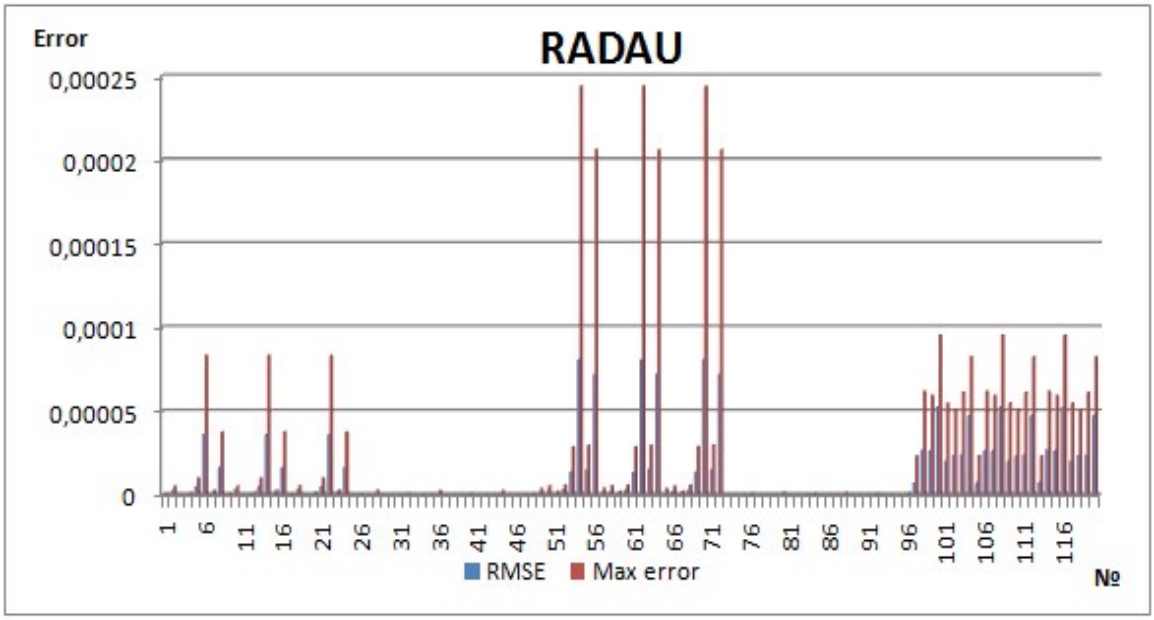

Figure 4: Histogram of RMSE and MaxError for RADAU
Source: created by the author

Figure 4 shows the histograms of RMSE and MaxError for the RADAU method. These graphs show the best stability among the considered methods. Single jumps when using Model 3 do not affect the overall accuracy. In particular, the peak values of RADAU errors are the lowest when using Model 3.

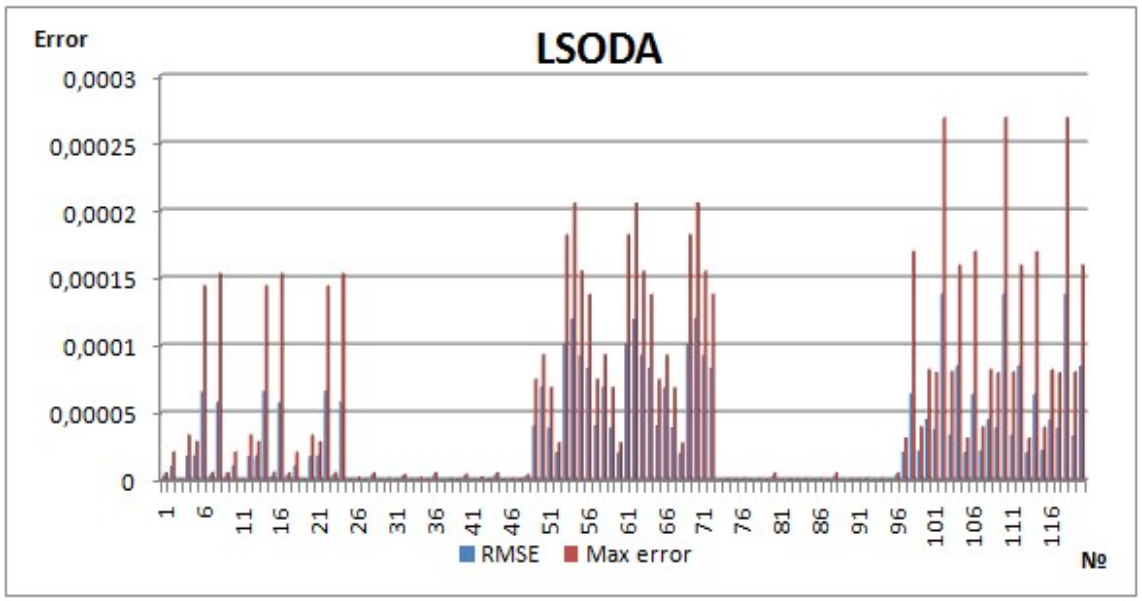

Figure 5: Histogram of RMSE and MaxError for LSODA
Source: created by the author

RMSE and MaxError for the LSODA method (Fig. 5) have an increase when using models 1, 3, and 5, but with a smaller amplitude than for the RK23 and BDF methods. However, these graphs are less stable than the RADAU

graphs. When using Model 3, LSODA has a significantly smaller error amplitude than RK23.

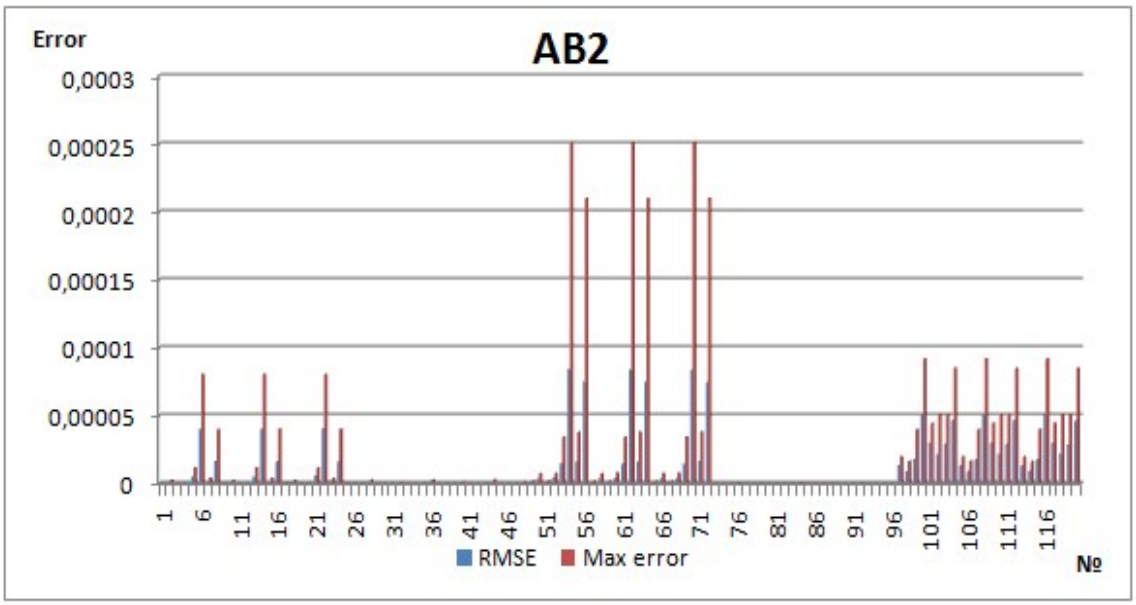

Figure 6: Histogram of RMSE and MaxError for AB2
Source: created by the author

Figure 6 shows histograms of the RMSE and MaxError metrics of the AB2 method. They are similar to the histograms of the RADAU method. But they have a higher frequency of increases in values for Model 5. And they do not have any increases for models MeanField_2 and MeanField_4_1.

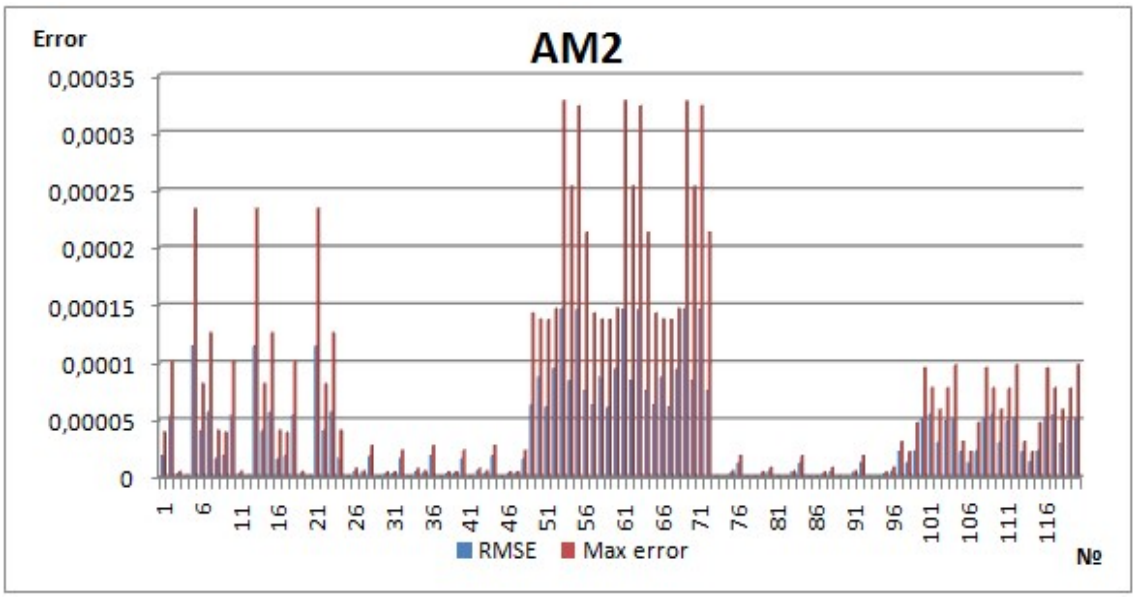

Figure 7: Histogram of RMSE and Max Error for AM2
Source: created by the author

The graphs of RMSE and MaxError values of the AM2 method (Figure 7) have sharp increases when using Models 1, 3, and 5. However, these increases occur with a much higher frequency than in the RADAU and AB2 methods, but the results of AM2 are better than LSODA. In general, increases

in RMSE and MaxError values are observed for most methods when using models with exponential infection, quadratic recovery rate, and exponential infection with rapid spread. This may be explained by the complicated dynamics of the system, which is created by nonlinear dependencies between variables. In particular, the exponential function on the right-hand side of the differential equation leads to a rapid increase in derivatives in response to even small changes in the number of infected units.

In the case of models with quadratic recovery rate, even moderate values of the number of infected units can lead to a large value of the rate of change. This complicates the approximation of the function and leads to the accumulation of errors at each integration step. The exponential nonlinearity in the infection model, especially at high values of k, simulates extremely fast infection. This requires the numerical algorithm to control the time step and high stability to rapid changes in the system's behaviour.

So, the features of the nonlinear structure of the models significantly affect the accuracy of the numerical solution. This confirms the need for a flexible choice of numerical method according to the class of the model, as well as the importance of a preliminary analysis of the sensitivity to model parameters and the equations' stiffness.

5. DISCUSSION

In this study, several MeanField-type models, including epidemiological analogues (SIR, SAEIQRS, etc.), were selected and adapted to most adequately describe the processes of threat propagation in networks. The test results confirm that such models take into account both the dynamics of infection and recovery in complex networks.

A large-scale comparison of the accuracy, speed, and stability of various methods, including RK4, DTM, VIM, and homotopy-based approaches, was conducted for nonlinear cyber threat models. The results showed that the choice of the optimal method significantly depends on the type of model, its rigidity, and the characteristics of the network topology.

The developed environment includes 120 scenarios with variations in infection, recovery, and network scale parameters. This gave grounds to assess the impact of topological changes on the accuracy of predictions and provide recommendations on the choice of a numerical method for specific cyberthreat conditions.

So, all research objectives were fulfilled, and the results confirm the practical applicability of the developed approach to modelling the spread of threats in information networks.

Unlike most previous studies that focused either on the creation of new numerical methods [8], [9] or on the analysis of individual specific models [13], [16], our study combines a systematic comparison of a wide range of numerical methods with an analysis of their performance on different variations of MeanField-type models. This approach identifies patterns between the class of the model, the features of its solution, and the achievable accuracy, which has not been implemented in similar studies so far.

In [20], the variational iteration method was applied to a modified epidemiological model of computer viruses, but without comparing it with other numerical approaches and without taking into account the real network topology. We not only compared this method with others (DTM, RK4, etc.) on identical and extended scenarios, but also integrated a dynamic network model and evaluated the effectiveness of the methods in more realistic conditions.

The study [21] is reduced to testing the DTM and RK4 methods for the SAEIQRS model, without taking into account the complexity of network dynamics and other classes of numerical methods. We applied 120 variations of scenarios with varying infection rates, recovery rates, network scale, and types of nonlinearities, which enabled providing more universal recommendations.

In [12], the focus is on the conceptual application of SIR models in cyber threats without deep numerical analysis. We extend this approach by adapting nonlinear models to a dynamic network and conducting a comprehensive computational experiment to assess accuracy, stability, and performance.

In [15], the spread of malware is modelled without taking into account changes in network topology. We used block models that reflect the time-varying structure of connections, which is close to real network traffic conditions.

In [10], a semi-analytical method based on homotopy analysis is proposed, but it is limited by mathematical correctness without verification in simulation scenarios. We evaluated not only the mathematical correctness, but also the behaviour of the methods in variational scenarios with different stiffness of the equations.

The study [14] considers the application of neural networks, but does not analyse the stability of classical numerical methods, which remain the

basis of real cyber defence systems. We partially closed this gap by providing recommendations for the choice of method depending on the model structure.

The research [11] presents probabilistic approaches to DR modelling, but without assessing the time efficiency. We showed how the speed of the method depends on the model class, and quantified this dependence.

In [19], the authors describe the mechanisms of infection but do not analyse numerical accuracy. We evaluated the accuracy using RMSE and MaxError, which are critical for risk prediction systems.

The study [22] focuses on the theoretical analysis of global stability, but without practical recommendations for the choice of method. We not only determined the conditions for the rigidity of the models, but also proposed adequate numerical methods for such cases.

Therefore, our study differs from existing studies as it combines the first-ever extensive testing of classical and modern numerical methods, consideration of network dynamics, and a comprehensive quantitative assessment of accuracy, speed, and stability. This gives grounds to provide practical recommendations for integration into cyber defence systems aimed at early detection and containment of cyber threats in real time.

So, the results of our study confirm the hypothesis that the accuracy and speed of the numerical method largely depend on the structure of nonlinearities in the model and the characteristics of the network. The practical value of the results is the possibility of integrating the recommendations for choosing a method for a specific type of threat and model into cyber defence systems. In particular, they can be used for early prediction of a malware epidemic or adaptive control of security policies in real time.

5.1. Limitations

The study focused on dynamic topologies with a limited class of models of the MeanField type, in particular only on single-component nonlinearities. Mostly classical numerical methods were used, although adaptive, stochastic and neural network numerical schemes are actively studied in current approaches. Furthermore, even despite the use of networks up to 10,000 nodes, real information systems can be much larger. They may also involve interaction with multiple attack types, which was not considered within the scope of this study.

5.2. Recommendations

It is appropriate to extend the considered models to the cases of stochastic or fractional DEs, which will allow for a more accurate description of complex attacks with random time parameters. Further improvement of network environment models may include adaptive topology change and simulation of cooperative attacks. Besides, modelling of systems with many types of users having different access levels and degrees of vulnerability, is promising.

5.3. Problems and open research issues

The conducted research assessed the effectiveness of numerical and semi-analytical methods for modelling the spread of cyber threats based on nonlinear differential equations in combination with realistic network topology models. At the same time, several problems were identified during the study that remain unresolved and form promising areas for further research:

1. The current sample of cyberthreat propagation scenarios does not cover the full range of possible attacks and network configurations. This limits the generalizability of the conclusions and requires the expansion of the database through simulation and experimental cases with different topologies, densities of connections, and levels of heterogeneity of nodes.
2. Despite taking into account certain features of the topology, the issues of realistic reproduction of large, multi-level, and dynamically changing networks remain open. Efficient algorithms for generating and processing such topologies in combination with DR models that take into account structural complexity are needed.
3. Current models mostly describe fixed patterns of infection and recovery. An open question is how to integrate the adaptive behaviour of attack and defence mechanisms that change over time, and how this affects network resilience.
4. Although accuracy and performance were analysed, there is still a need for a comprehensive multi-criteria evaluation that also takes into account stability, scalability, and sensitivity to model parameters.
5. A potential direction of development is the combination of numerical methods for solving DR with machine learning algorithms for automatic adjustment of model parameters, anomaly detection, and prediction of threat evolution in real time.

6. CONCLUSIONS

This study aimed to compare and analyse the effectiveness of numerical methods for solving nonlinear differential equations (DEs) describing the propagation of threats in induced networks (INs) in order to determine the most accurate, fast, and stable approaches for practical application in modelling and ensuring cybersecurity.

The aim was achieved through the fulfilment of the following research objectives:

- a review of current approaches to mathematical modelling of cyber threats using DR was performed;
- the most common types of nonlinear models were identified, in particular, models based on MeanField with exponential, logarithmic, and power dependences;
- seven numerical methods (Radau, AB2, LSODA, BDF, AM2, etc.) were implemented and tested on a wide range of scenarios;
- a software mathematical platform was created for modelling and analysing threat propagation processes in dynamic networks.

The results of the study:

Radau and AB2 showed the highest accuracy (10^{-5}…10^{-7}) at relatively low computational costs;

LSODA provided the optimal balance between accuracy and performance, which makes it a practical choice for a wide class of problems;

BDF and AM2 were less effective for hard problems with high model complexity or a large value of the infection parameter;

Sensitivity analysis showed that the accuracy of the methods decreases with increasing infection rate (β) and increases with a higher recovery rate (γ);

Increasing the network size by 10 times did not lead to a significant deterioration in the results, which indicates the scalability of the approach.

The academic contribution of the study is in the first-ever comprehensive testing of classical and modern numerical methods on different variations of nonlinear models in the context of cyber threats, taking into account the dynamics of the network topology and a wide range of parameters. The obtained results gave grounds to provide practical recommendations for choosing a numerical method depending on the characteristics of the model, the level of rigidity of the equations, and the requirements for speed.

The practical significance is the possibility of integrating the developed models and algorithms into early warning systems, automated response, and adaptive security management in real time, which is especially relevant for critical infrastructure.

Further research directions:

- adaptation of the platform to the analysis of real networks based on empirical data;
- integration of fuzzy logic methods for adaptive identification of threat parameters;
- expansion of mathematical models by taking into account latent states, interconnected networks, and hybrid attacks;
- research into hybrid approaches that combine numerical methods with machine learning to increase the forecasting accuracy and speed.

So, the study not only confirmed the hypothesis that the accuracy and speed of numerical methods depend on the structure of nonlinearities and network characteristics, but also provided practical tools for modelling and assessing cyber threats in scalable networks.

REFERENCES

[1] M. A. Bouke and A. Abdullah, "Smrd: A novel cyber warfare modeling framework for social engineering, malware, ransomware, and distributed denial-of-service based on a system of nonlinear differential equations," *Journal of Applied Artificial Intelligence*, Vol. 5, No. 1, 2024, pp. 54-68, doi: 10.48185/jaai.v5i1.972.

[2] G. G. Mohammed and Z. Zaheer, "NeuroCyberGuard: Developing a Robust Cybersecurity Defense System through Deep Neural Learning-Based Mathematical Modeling," *Journal of Smart Internet of Things*, Vol. 2022, No. 1, 2022, pp. 133-145, doi: 10.2478/jsiot-2022-0009.

[3] H. Durand, "A nonlinear systems framework for cyberattack prevention for chemical process control systems," *Mathematics*, Vol. 6, No. 9, 2018, pp. 169.

[4] M. Belova, V. Denysenko, S. Kartashova, V. Kotlyar and S. Mikhailenko, "Analysis of the Structure of Chaotic Solutions of Differential Equations," *WSEAS Transactions on Circuits and Systems*, Vol. 22, 2023, pp. 75-85, doi: 10.37394/23201.2023.22.10.

[5] F. K. Batista, Á. Martín del Rey, S. Quintero-Bonilla and A. Queiruga-Dios, "A SEIR Model for Computer Virus Spreading Based on Cellular Automata," *Advances in Intelligent Systems and Computing*, Vol 649. 2018, doi: 10.1007/978-3-319-67180-2_62.

[6] G. Manohara and S. Kumbinarasaiah, "Numerical solution of a modified

epidemiological model of computer viruses by using Fibonacci wavelets," *The Journal of Analysis,* Vol. 32, 2024, pp. 529–554, doi: 10.1007/s41478-023-00663-7.

[7] M. Belova, V. Denysenko, S. Kartashova, V. Kotlyar, S. Mikhailenko, "Study of the Impact of Loads on the Deformation of Building Structures using Differential Equations," *WSEAS Transactions on Systems,* Vol. 23, 2024, pp. 398-408, doi: 10.37394/23202.2024.23.42.

[8] S. Kaushik and R. Kumar, "Qualitative Analysis of a Novel Numerical Method for Solving Non-linear Ordinary Differential Equations," *International Journal of Applied and Computational Mathematics,* Vol. 10, 2024, pp. 99, doi: 10.1007/s40819-024-01735-3.

[9] Z. Odibat, "An improved optimal homotopy analysis algorithm for nonlinear differential equations," *Journal of Mathematical Analysis and Applications*, Vol. 488, Iss. 2, 2020, pp. 124089, doi: 10.1016/j.jmaa.2020.124089.

[10] S. Hussain, G. Arora and R. Kumar, "Semi-analytical methods for solving non-linear differential equations: A review," *Journal of Mathematical Analysis and Applications*, Vol. 531, Iss. 1, Part 2, 2024, pp. 127821, doi: 10.1016/j.jmaa.2023.127821.

[11] J. Wang, J. Cockayne, O. Chkrebtii T. J. Sullivan and C. J. Oates, "Bayesian numerical methods for nonlinear partial differential equations," *Statistics and Computing,* Vol. 31, 2021, pp. 55, doi: 10.1007/s11222-021-10030-w.

[12] M. T. Gençoğlu, "Mathematical Modeling in Cyber Defense," *International Journal of Engineering Science and Application,* Vol. 4, No. 4, 2020, pp. 165-169.

[13] Z. Wang, L. Chen, S. Song, P. X. Cong and Q. Ruan, "Automatic cyber security risk assessment based on fuzzy fractional ordinary differential equations," *Alexandria Engineering Journal,* Vol. 59, Iss. 4, 2020, pp. 2725-2731, doi: 10.1016/j.aej.2020.05.014.

[14] P. Sungu Ngoy, K. Musumbu and D. Kioi, "A Mathematical Modeling Approach in Cybersecurity using Deep neural Learning," *International Journal of Advanced Research in Science, Engineering and Technology*, Vol. 8, Iss. 6, 2021.

[15] J. Johnson, "A Dynamical Systems Approach for Modeling Malware Propagating Through a Network and Potential Solutions Towards Mitigating Spread," *2024 Fall Cybersecurity Undergraduate Research Projects*, 2024, doi: 10.25776/2dzk-hr66.

[16] H. Zhang, Y. Mi, Y. Fu, X. Liu, Y. Zhang, J. Wang and J. Tan, "Security defense decision method based on potential differential game for complex networks," *Computers & Security,* Vol. 129, 2023, pp. 103187, doi: 10.1016/j.cose.2023.103187.

[17] R. Hryshchuk, "Example of Differential Transformations Application in Cybersecurity." *ISecIT*, 2021, pp. 223-227.

[18] S. Wu, "Nonlinear information data mining based on time series for fractional differential operators," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, Vol. 29, No. 1, 2019, doi: 10.1063/1.5085430.

[19] N. Levy, A. Rubin and E. Yom-Tov, "Modeling infection methods of computer malware in the presence of vaccinations using epidemiological models: an analysis of real-world data," *International Journal of Data Science and Analytics,* Vol. 10, No. 4, 2020, pp. 349-358.

[20] S. Noeiaghdam, "A novel technique to solve the modified epidemiological model of computer viruses," *SeMA Journal*, Vol. 76, No. 1, 2019, pp. 97-108.

[21] P. Shahrear, A. K. Chakraborty, Md. A. Islam and U. Habiba, "Analysis of computer virus propagation based on compartmental model," *Applied and Computational Mathematics*, Vol. 7, No. 1-2, 2018, pp. 12-21.

[22] M. T. Hoang, "Global asymptotic stability of some epidemiological models for computer viruses and malware using nonlinear cascade systems," *Boletín de la Sociedad Matemática Mexicana,* Vol. 28, 2022, pp. 39, doi: 10.1007/s40590-022-00432-9.

[23] S. Noeiaghdam, M. Suleman and H. Budak, "Solving a modified nonlinear epidemiological model of computer viruses by homotopy analysis method," *Mathematical Sciences,* Vol. 12, 2018, pp. 211–222, doi: 10.1007/s40096-018-0261-5.

[24] M. Izadi, M. Seifaddini and M. Afshar, "Approximate solutions of a SIR epidemiological model of computer viruses," *Tbilisi Mathematical Journal*, Vol. 14, No. 4, 2021, pp. 203-219.

[25] A. Martín Del Rey, R. C. Vara and S. Rodríguez González, "A computational propagation model for malware based on the SIR classic model," *Neurocomputing*, Vol. 484, 2022, pp. 161-171.

[26] S. Ottaviano and S. Bonaccorsi, "Some aspects of the Markovian SIRS epidemic on networks and its mean-field approximation," *Mathematical Methods in the Applied Sciences*, Vol. 44, No. 6, 2021, pp. 4952-4971.

[27] E. Tadmor, "On the stability of Runge–Kutta methods for arbitrarily large systems of ODEs," *Communications on Pure and Applied Mathematics*, Vol. 78, No. 4, 2025, pp. 821-855, doi: 10.1002/cpa.22238.

[28] S. Ekanathan, O. Smith and C. Rackauckas, "A Fully Adaptive Radau Method for the Efficient Solution of Stiff Ordinary Differential Equations at Low Tolerances," *arXiv preprint arXiv:2412.14362*, 2024.

[29] S. Rathan, D. Shah, T. H. Kumar and K. S. Charan, "Adaptive IQ and IMQ-RBFs for Solving Initial Value Problems: Adams–Bashforth and Adams–Moulton Methods," *International Journal of Computational Methods*, Vol. 21, No. 03, 2024, pp. 2350032.