

STRATEGIES FOR ENSURING FUNCTIONAL STABILITY OF A COMPLEX SENSOR NETWORK BASED ON THE RESEARCH OF THE DYNAMICS OF THE BEHAVIOUR OF EVOLUTIONARY EQUATIONS

Valentyn Sobchuk¹, Yurii Kravchenko¹, Mykhaylo Sharapov¹, Oleksandr Laptiev¹, Andrii Sobchuk²

¹Taras Shevchenko National University of Kyiv, Kyiv, Ukraine, ²State University of Information and Communication Technologies, Kyiv, Ukraine

Abstract: Wireless sensor networks play an increasingly important role in navigation and monitoring tasks in modern conflict environments, where their operation is continuously affected by destabilizing external and internal factors. Ensuring the functional stability of such networks under sustained adverse influence therefore represents a critical scientific and practical problem. This paper develops a mathematically grounded framework for analyzing and maintaining the functional stability of a complex wireless sensor network operating under risk exposure. The qualitative theory of differential equations is applied to describe and characterize the state of the system under such conditions. To mathematically formalize the behavior of the sensor network, the classical evolutionary SIR model is employed, and constructive conditions for network stability and asymptotic stability are formulated. Three functional stability strategies – constant monitoring, impulsive recovery, and periodic recovery – are formally introduced and analyzed within a unified modeling framework. For each strategy, explicit conditions are obtained under which the number of compromised network nodes asymptotically decreases, ensuring the preservation of network functionality. The effects of recovery and restoration actions are analyzed using phase-plane methods. The dependence of network stability on model parameters describing node compromise, attrition, and recovery rates is established, and an analytical model for determining the time required to restore functional stability is derived. The resulting mathematical framework provides a rigorous theoretical basis for selecting and comparing functional stability strategies for wireless sensor networks operating under persistent destabilizing conditions.

Keywords: wireless sensor networks, functional stability assurance, SIR model, system of differential equations with impulsive action, state-dependent impulsive control

STRATEGIE ZAPEWNIENIA FUNKCJONALNEJ STABILNOŚCI ZŁOŻONEJ SIECI SENSOROWEJ NA PODSTAWIE BADAN DYNAMIKI ZACHOWANIA RÓWNAŃ EWOLUCYJNYCH

Streszczenie. Bezprzewodowe sieci sensorowe odgrywają coraz istotniejszą rolę w realizacji zadań nawigacyjnych i monitorujących w warunkach współczesnych konfliktów, gdzie ich funkcjonowanie jest nieustannie narażone na oddziaływanie destabilizujących czynników zewnętrznych i wewnętrznych. Zapewnienie funkcjonalnej stabilności takich sieci w warunkach długotrwałego wpływu stanowi zatem istotny problem naukowy i praktyczny. W niniejszej pracy opracowano matematycznie podstawy analityczne służące do analizy i utrzymania funkcjonalnej stabilności złożonej bezprzewodowej sieci sensorowej działającej w warunkach ekspozycji na ryzyko. Do opisu i charakterystyki stanu systemu w takich warunkach zastosowano aparat jakościowej teorii równań różniczkowych. W celu matematycznej formalizacji zachowania sieci sensorowej wykorzystano klasyczny ewolucyjny model SIR oraz sformulowano konstruktywne warunki stabilności i asymptotycznej stabilności sieci. W ramach jednolitego modelu formalnie wprowadzono i przeanalizowano trzy strategie zapewnienia funkcjonalnej stabilności: stały monitoring, odtwarzanie impulsowe oraz odtwarzanie okresowe. Dla każdej strategii określa się konkretne warunki, w których liczba zaatakowanych węzłów sieciowych asymptotycznie maleje, co gwarantuje zachowanie funkcjonalności sieci. Wpływ działań naprawczych i odwrócenia uszkodzeń przeanalizowano z wykorzystaniem metod płaszczyzny fazowej. Wykazano zależność stabilności sieci od parametrów modelu opisujących tempo naruszenia bezpieczeństwa węzłów, ich utratę oraz tempo przywrócenia sprawności, a także opracowano model analityczny służący do określania czasu niezbędnego do przywrócenia stabilności funkcjonalnej. Opracowane ramy matematyczne stanowią rygorystyczną podstawę teoretyczną do doboru i porównywania strategii zapewnienia funkcjonalnej stabilności bezprzewodowych sieci sensorowych działających w warunkach trwałego oddziaływania czynników destabilizujących.

Słowa kluczowe: bezprzewodowe sieci sensorowe, zapewnienie stabilności funkcjonalnej, model SIR, układ równań różniczkowych z działaniem impulsowym, sterowanie impulsowe zależne od stanu

Introduction

One of the foremost directions in contemporary information technology is the rapid advancement of wireless sensor networks, which are being extensively deployed across diverse application domains [9].

In the current complex political and military environment, the implementation and continued utilization of such networks in the defence sector is of particular significance for Ukraine as well as for other states, including NATO member countries. Wireless sensor networks are employed to address critical tasks of navigation and battlefield monitoring – functions that are of paramount importance to military stakeholders [19].

Solving these tasks enables the formation of an advantage in situational awareness and the effective coordination of actions, reduces decision-making time, mitigates risks and losses, and ensures operational capability under conditions of uncertainty and adversarial influence.

Integrated systems for terrain monitoring and autonomous navigation are capable of fulfilling a broad spectrum of functional objectives. However, under actual battlefield conditions, such systems are inevitably subject to destabilizing factors, including active adversary measures directed at disabling specific network components or disrupting the overall operation of the system.

To mitigate potential adverse impacts, such systems must exhibit adaptive behaviour – most notably, the capacity to transition from passive to active modes in response to variations in the external environment. This adaptability enables the preservation of core functionality even under conditions of partial destruction or intentional interference.

Accordingly, the study of the behavioural characteristics of complex systems under destabilizing conditions is highly relevant, as it provides the foundation for the development of effective strategies to ensure their functional stability in the face of real-world threats.

Objective statement. The objective of this study is to investigate the dynamic behaviour of wireless sensor networks operating under persistent destabilizing influences and to develop analytically grounded strategies for maintaining their functional stability under such conditions.

To achieve this objective, the network degradation and recovery processes are modelled using a system of evolutionary differential equations of the SIR type, which describe transitions between susceptible, compromised, and recovered states of network components. The qualitative theory of differential equations and phase-plane analysis are employed to analyse system trajectories, identify stability conditions, and evaluate the impact of different recovery and monitoring strategies on long-term network functionality.



1. Related works

The problem of ensuring the functional stability of complex technical systems, including information systems as one of their varieties, has consistently attracted the attention of numerous researchers. In [3], a broad range of issues related to ensuring the functional stability of information systems under the influence of destabilizing factors is discussed.

A methodology for ensuring the functional stability of an information system within critical infrastructure facilities through a formalized process of self-testing is proposed in [2]. The primary procedures for maintaining the functional stability of a network are continuous diagnostics aimed at detecting failed nodes and diagnosing compromised nodes in order to preserve the required parameters of the network's autonomous operation. A method of self-correction for an analogue-to-digital network based on current converters with weight redundancy is presented in [1]. In [13], anomaly detection in sensor networks using Fourier transformations is examined. The work in [5] investigates the application of machine learning methods – specifically, random forests and rule-based systems – for detecting malicious processes in information networks.

An adaptive self-diagnosis method for networks based on the functional relationship between the probability of missed failures and various values of the type II error probability is presented in [4]. More in-depth analyses of corresponding results for complex sensor networks can be found in [7, 8]. Methods for ensuring the stable operation of a wireless wide area network using a neuro-fuzzy controller are discussed in [15]. A method for parametric diagnostics of the functional stability of a mechanical system employing fuzzy logic is proposed in [16].

The methods proposed in these works play a key role in ensuring the reliable functioning of information networks exposed to diverse risks. At the same time, these studies are largely based on the application of probability theory to the mathematical formalization of network functioning. However, the problem of establishing the dependence of risk growth on time and on the dynamics of sensor network functioning under risk factors remains almost entirely unexplored.

The application of the evolutionary SIR model [10, 12] makes it possible to investigate the state of a complex system in dynamics. In [14], the author demonstrates that the use of this model is promising for describing phenomena occurring in complex systems beyond epidemiology – in finance, social networks, cybersecurity, and even science fiction.

Within the framework of the epidemiological model, vaccination serves as a method of counteraction and influence on the dynamics of epidemic progression in a complex system. The works [6, 11, 17, 18, 20] analyse the impact and effectiveness of various vaccination strategies and approaches. In [9], it is demonstrated that the theory of differential equations with impulsive action can be employed for the purposes of formalizing and analysing dynamics.

2. Representing the stability of a sensor network using the SIR model

In the context of the ongoing acute phase of armed aggression in Ukraine, the issue of ensuring the functional stability of complex information systems, which are widely employed in modern warfare, becomes particularly relevant. We live in conditions of a high concentration of diverse complexes, which, on the one hand, constantly rely on a large number of devices with varying degrees of autonomy to perform both offensive and defensive combat tasks. Consequently, the line of contact in today's armed conflict can de facto be viewed as a complex heterogeneous network that is continuously exposed to external and internal destabilizing factors of diverse nature. The entire technical and technological arsenal of these networks thus operates under the influence of numerous risks of damage, destruction, and other forms of degradation.

Let us analyse the main risks to which wireless sensor network devices along the line of contact are subjected. These risks can conventionally be classified as physical, cyber, electromagnetic, and operational, as presented in Table 1.

Recovery actions to mitigate the aforementioned risks can be summarized as follows:

- reconfiguration,
- reinstallation of software,
- repair,
- replacement.

Table 1. Characteristics of risks affecting wireless sensor network devices on the line of contact

Subgroup	Risk	Immediately detectable?	Possible response
Physical	1. Device destruction	Yes	Replacement
	2. Device damage	Not always	Repair/ Replacement
Electromagnetic	3. Channel jamming	Not immediately	Reconfiguration of frequency/protocol
	4. Spoofing (false signal injection)	No	Source verification/ Filtering
Cyber	5. Malware injection	No	Reinstallation/ Isolation
Operational	6. Battery depletion	Often – No	Power replacement
	7. Software malfunction	Not always	Restart/Reflash
	8. Loss of connectivity with other nodes	Not immediately	Reconfiguration/ Route bypass

In this work, we consider the modelling of evolutionary processes for ensuring the functional stability of a complex wireless sensor network for monitoring and navigation along the line of contact, taking into account the effects of damage and recovery factors, using the framework of qualitative theory of nonlinear differential equations.

The most natural mathematical formalization for describing evolutionary processes induced by direct anthropogenic and natural influences appears to us to be the SIR model [10, 12, 14]. The SIR evolutionary model will be employed not merely as a descriptive tool, but as a formal mechanism for constructing and evaluating functional stability strategies under sustained destabilizing influence.

We now examine the mathematical aspects of the classical SIR model, incorporating a "vaccination procedure" to model the evolution of the sensor network state. Let the set of network devices (nodes) be divided into three groups:

$S(t)$ – nodes susceptible to damage, including those potentially known to the adversary but not yet affected at a given time; $I(t)$ – affected nodes; $R(t)$ – recovered nodes that are temporarily resistant to re-infection.

We further assume that all three groups represent fractions of the total segmented network population, so these values are normalized and their sum equals one.

For simplicity, we also assume that the time required for node recovery is negligible compared to its operational lifetime and can therefore be ignored.

It should be noted that the sensor network functions as a dynamic system in which there are processes of node attrition and replenishment with new devices, analogous to processes observed in natural populations. The mathematical model of the network's functioning can thus be expressed as a system of nonlinear differential equations:

$$\begin{cases} \frac{dS(t)}{dt} = -\lambda S(t)I(t) + \mu - \mu S(t) \\ \frac{dI(t)}{dt} = \lambda S(t)I(t) - \gamma I(t) - \mu I(t) \end{cases} \quad (1)$$

It should be noted that the following condition holds:

$$R(t) = 1 - S(t) - I(t)$$

In system (1) $\lambda > 0$ is a parameter characterizing the rate at which nodes transition from the susceptible class to the affected ("infected") class; $\mu > 0$ – is a parameter representing the attrition of nodes due to adverse factors (this same parameter also reflects the appearance of new nodes in the network, effectively capturing

the "birth/death" dynamics of its nodes); $\gamma > 0$ – is a parameter describing the intensity of node recovery.

The relationships among these parameters collectively characterize the network's resilience to threats and govern its dynamic behaviour. Specifically, the ratio of the rate of node susceptibility to the rates of node attrition and recovery serves as a bifurcation parameter, determining the evolutionary processes within the network. We denote this parameter as:

$$\delta = \frac{\lambda}{\gamma + \mu}$$

By employing the methods of the qualitative theory of differential equations, we can obtain essential insights into the behaviour of the system that cannot be derived solely through analytical solution techniques. This information may then be used for prediction, analysis, and system design.

In particular, the methods of qualitative theory allow us to determine what types of trajectories exist in the system's phase space, how they are arranged, and how they interact with one another. These methods enable the identification of stationary points, repellers and attractors, and periodic trajectories. Furthermore, they make it possible to assess whether the system is stable – that is, whether its trajectories remain close to the initial trajectory under small perturbations of the initial conditions. Of significant practical importance is also the ability to predict how the qualitative behaviour of the system changes as its parameters vary.

Thus, the qualitative theory of evolutionary equations can serve as an effective tool not only for forecasting the vulnerabilities of a sensor network to adverse factors but also for developing strategies of counteraction and sustaining the functionality of the network.

We now proceed to investigate the qualitative behaviour of system (1) in the domain:

$$\mathcal{D} = \{(S, I) \mid S \geq 0, I \geq 0, S + I \leq 1\}$$

System (1) admits two equilibrium points. In the *SOI* phase plane we distinguish them as follows:

- **"Infection free" equilibrium point:** $S_0^* = 1, I_0^* = 0$ – corresponding to the state without impairments (i.e., no signs of vulnerability under adverse factors);
- **"Epidemic" equilibrium point:** $S_1^* = \frac{1}{\sigma}, I_1^* = \frac{\mu(\delta-1)}{\lambda}$ – representing the situation in which a threshold proportion of network devices becomes vulnerable (an analogue of reaching the epidemic threshold in infectious disease dynamics within anthropogenic populations).

Under these circumstances, the qualitative behaviour of system (1) is determined by the value of the parameter δ . Theorem holds.

Theorem 1. [6] For $\forall \delta > 0$ the domain $\mathcal{D}$ is invariant, i.e. $\forall (S_0, I_0) \in \mathcal{D}$ the solution of system (1) $(S(t), I(t))$ with initial conditions $S(0) = S_0, I(0) = I_0$ remains in $\mathcal{D}, \forall t \geq 0$, that is, $(S(t), I(t)) \in \mathcal{D}, \forall t \geq 0$.

For $\forall \delta > 0$, system (1) has no closed trajectories in $\mathcal{D}$.

For $\delta \leq 1$ the point (S_0^*, I_0^*) is a globally asymptotically stable equilibrium in $\mathcal{D}$ (Note: in this case $(S_1^*, I_1^*) \notin \mathcal{D}$) (Fig 1a).

For $\delta > 1$, the point (S_0^*, I_0^*) is an unstable equilibrium in $\mathcal{D}$ (the only trajectory attracted to (S_0^*, I_0^*) – is given by $I(t) \equiv 0, S(t) = (S_0 - 1)e^{-\mu t} + 1$). The point (S_1^*, I_1^*) is an asymptotically stable equilibrium with the domain of attraction $\mathcal{D} \setminus \{(S, 0) \mid 0 \leq S \leq 1\}$ (Fig 1b).

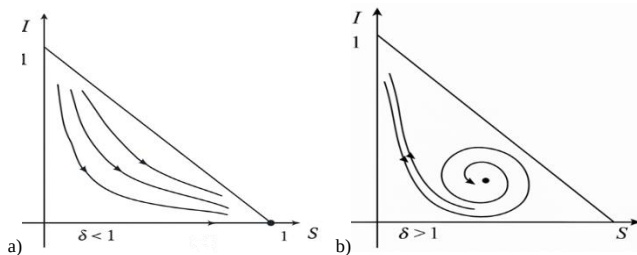


Fig. 1. Phase portrait of system (1)

Thus, we can state that when the parameter $\delta \leq 1$, regardless of the initial conditions, the number of compromised devices decreases over time to an arbitrarily small level. In contrast, for $\delta > 1$ we observe a situation of critical compromise, where the system evolves toward the threshold number of compromised devices in the network (S_1^*, I_1^*) , which constitutes an asymptotically stable equilibrium point with the domain of attraction $\mathcal{D} \setminus \{(S, 0) \mid 0 \leq S \leq 1\}$.

According to the conditions of Theorem 1, the invariance of the domain $\mathcal{D}$ allows us to conclude that such behaviour is characteristic of any network, since no assumptions were made about the specific properties or parameters of the devices comprising the network.

For the practical development of strategies to counteract negative impacts on the sensor network, it is necessary to address the following question: *how can the level of compromised nodes be reduced when $\delta > 1$?*

I. Constant vaccination strategy. This approach involves establishing a systematic monitoring framework for the network nodes that can identify and neutralize threats in real time (serving as an analogue to the vaccination of new-borns in anthropogenic systems). If we denote by p the fraction of network devices under such constant monitoring, then for $\delta > 1$ we obtain the following system:

$$\begin{cases} \frac{dS(t)}{dt} = (1-p)\mu - (\lambda I(t) + \mu)S(t) \\ \frac{dI(t)}{dt} = \lambda S(t)I(t) - (\gamma + \mu)I(t) \end{cases} \quad (2)$$

The equilibrium states of system (2) are as follows:

$$\begin{aligned} \hat{S}_0^* &= 1 - p, \quad \hat{I}_0^* = 0 \\ \hat{S}_1^* &= \frac{1}{\sigma}, \quad \hat{I}_1^* = I_1^* - \frac{\mu}{\mu + \gamma} p \end{aligned}$$

The qualitative behaviour of system (2) is determined by a certain threshold value of the parameter $p_* = 1 - \frac{1}{\delta}$.

Theorem 2. [11] For $\forall p \in (0, 1)$, the domain $\mathcal{D}$ is invariant in system (2). Within the domain $\mathcal{D}$ there are no closed trajectories of system (2).

When $p > p_*$ the point $(\hat{S}_0^*, \hat{I}_0^*)$ is an asymptotically stable equilibrium in $\mathcal{D}$; whereas $(\hat{S}_1^*, \hat{I}_1^*)$ is an unstable equilibrium.

When $p < p_*$ the point $(\hat{S}_0^*, \hat{I}_0^*)$ is an unstable equilibrium in domain $\mathcal{D}$; $(\hat{S}_1^*, \hat{I}_1^*)$ is an asymptotically stable equilibrium.

Thus, stability – and, consequently, the resilience of the network for $p > p_*$ is ensured at the point $(\hat{S}_0^*, \hat{I}_0^*)$, while for $p < p_*$ it is realized at the point $(\hat{S}_1^*, \hat{I}_1^*)$. However, in the situation where $p > p_*$ in the neighbourhood of $(\hat{S}_1^*, \hat{I}_1^*)$ and where $p < p_*$ in the neighbourhood of $(\hat{S}_0^*, \hat{I}_0^*)$ stability with respect to harmful impacts is lost, and the network itself is thus characterized by significant vulnerability. In such cases, it becomes necessary to adopt measures aimed at minimizing risks.

A major drawback of this strategy lies in its cost, since its implementation requires allocating system resources for continuous monitoring.

II. Pulse vaccination strategy. Applied to a human population, this strategy implies vaccinating a certain fraction of the population susceptible to infection at specific points in time. The network analogy is selective monitoring and recovery actions applied to potentially vulnerable segments of the network, i.e. $S(t)$. As a modelling abstraction, we also assume that recovery actions are performed over a negligible time span (i.e., instantaneously, in pulse form).

Let $\{t_n\}_{n=0}^{\infty}$ be the sequence of recovery action moments. Then, for $\delta > 1$ the problem takes the following form:

$$\begin{cases} \frac{dS(t)}{dt} = -\lambda S(t)I(t) + \mu - \mu S(t), & t \neq t_n \\ \frac{dI(t)}{dt} = \lambda S(t)I(t) - \gamma I(t) - \mu I(t), & t \neq t_n \\ \Delta S|_{t=t_n} := S(t_n + 0) - S(t_n - 0) = -\varphi(S(t_n - 0)) \end{cases} \quad (3)$$

$$\Delta S|_{t=t_n} := S(t_n + 0) - S(t_n - 0) = -\varphi(S(t_n - 0)) \quad (4)$$

We assume that $\varphi(S) \leq 0$ for $S \geq 0$, and we consider the function $S(t)$ to be right-continuous at the points $\{t_n\}$. Then, for system (3), (4), the qualitative behaviour depends on the impulse parameters $\{t_n\}$ and $\varphi(S)$.

Condition (4) constitutes a mathematical formalization of the recovery process, stipulating that after each such procedure the network evolves according to law (3) until the next scheduled maintenance and restorative procedure.

III. Periodic case. Let $t_n = nT$, $n = 0, 1, \dots$. In this case, it is assumed that restorative procedures are scheduled by regulation and possess a periodic nature with a prescribed period. We set:

$$\varphi(S) = -p \cdot S, \quad p \in (0, 1)$$

Then, particular significance is attached to the limiting number of nodes susceptible to compromise

$$S_* = \frac{(1-p)(e^{\mu T} - 1)}{p - 1 + e^{\mu T}}$$

The following theorem holds.

Theorem 3. [18] System (3), (4) admits a periodic impulsive solution ("infection-free" periodic solution) given by

$$\bar{S}(t) = \begin{cases} 1 + \frac{p \cdot e^{\mu T}}{1 - p - e^{\mu T}} \cdot e^{-\mu(t-t_n)} & t \in [t_n, t_{n+1}) \\ S_* & t = t_{n+1} \end{cases}$$

$$\bar{I}(t) \equiv 0$$

This solution is asymptotically stable under the condition

$$\frac{1}{T} \int_0^T \bar{S}(t) dt < \frac{1}{\delta} \quad (5)$$

Corollary. The functional stability reserve of a complex wireless sensor network for monitoring and navigation along the line of contact is inversely proportional to the ratio of the node compromise rate to the rates of node attrition and recovery, whose collective dynamics are governed by system (3), (4). This system admits an asymptotically stable impulsive periodic solution ("infection-free" periodic solution) provided that condition (5) is satisfied.

Specifically, condition (5) indicates that the network's stability to threats is inversely determined by the ratio of the node compromise rate to the rates of node attrition and recovery. In practice, the continuous replenishment of the network with new protected nodes ensures stable network operation over time, even in the presence of vulnerabilities in certain network segments.

The graph of $I(t)$, representing the dynamics of compromised nodes in the network with $I(0) = I_0 \in (0, 1)$ as $t \rightarrow \infty$ is shown in Figure 2. This illustrates that periodic monitoring and recovery actions progressively minimize the number of network devices affected by adverse factors, reducing it practically to zero over time. The non-monotonic, oscillatory behavior reflects alternating phases of degradation and intervention, while the decreasing envelope of the trajectory indicates asymptotic stabilization of the system under repeated recovery measures.

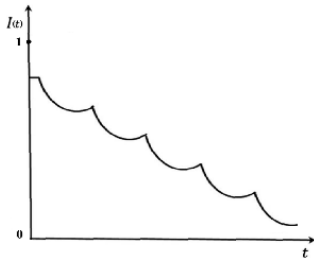


Fig. 2. Illustration of the dynamics of the fraction of compromised nodes $I(t)$, $I(0) = I_0 \in (0, 1)$ as time $t \rightarrow \infty$

We note that condition (5) can be expressed explicitly as

$$\frac{(\mu T - p)(e^{\mu T} - 1) + \mu p T}{\mu T(p - 1 + e^{\mu T})} < \frac{1}{\delta} \quad (6)$$

From Theorem 3 and formulas (5) and (6), we can draw an important conclusion.

Conclusion 1. If the period of monitoring and recovery actions satisfies

$$T < T_* = \frac{1}{\mu} \ln \left(1 + \frac{p}{\delta - p} \right) \quad (7)$$

then the condition $I(t) \rightarrow 0$, $t \rightarrow \infty$ will be fulfilled.

The problem of network evolution described by system (3) with impulsive recovery actions (4) can be generalized. It is therefore worthwhile to focus on the study of such problems.

Problem 1. Periodic recovery with "fuzzy" information on the number of updated network nodes: $t_n = nT$, $n = 0, 1, \dots$

$$\Delta S|_{t=t_n} \in [-\varphi_1(S(t_n - 0)), -\varphi_2(S(t_n - 0))]$$

where φ_1, φ_2 are given functions.

Problem 2. Almost periodic recovery: Let $\{t_n\}$ be quasi-periodic (i.e., close to periodic), such that $t_n = nT + \tau_n$, $\tau_n \in [0, T)$.

$$\Delta S|_{t=t_n} = -p \cdot S(t_n - 0)$$

Problem 3. Recovery with known statistical information on the number of updated network nodes: Let $\{t_n\}$ satisfy

$$\overline{\lim}_{\tau \rightarrow \infty} \frac{N(t, t + \tau)}{\tau} < \infty$$

where $N(t, t + \tau)$ is the number of update moments t_n in the interval $(t, t + \tau)$, and $\{p_n(\omega)\}$ are random variables with given probabilistic characteristics. Then,

$$\Delta S|_{t=t_n} = -p(\omega) \cdot S(t_n - 0)$$

The qualitative behaviour of system (3), (4) for Problems 1–3 will be investigated in subsequent studies in order to develop a comprehensive methodology for selecting effective strategies to ensure the functional stability of a complex wireless navigation and monitoring network.

1. Conclusion

Wireless sensor networks employed for navigation and monitoring along the line of contact provide a technical advantage over adversaries, which constitutes an integral component of modern defence capability and simultaneously contributes to enhancing national security.

To ensure the functional stability of complex information and communication systems for monitoring and navigation along the line of contact, such systems must be adaptive to the continuous influence of destabilizing factors of both external and internal nature. System adaptability implies the ability to select and implement appropriate strategies to restore basic functionality throughout the period during which the system is exposed to harmful factors.

This study develops and substantiates a mathematical framework for analysing and maintaining the functional stability of wireless sensor networks under adverse operating conditions. The behaviour of the network is described using systems of evolutionary differential equations with impulsive effects, and their qualitative properties are examined using phase-plane analysis and stability theory. In particular, by employing an evolutionary SIR model as a mathematical representation of the sensor network, constructive conditions for stability and asymptotic stability of such systems are derived.

We established conditions for preserving network functional stability through various strategies to minimize the number of compromised nodes: constant monitoring, impulsive recovery, and periodic recovery.

Furthermore, the dependence of network stability on model parameters describing the rates of node attrition and replacement/recovery is determined. A model for calculating the time required to restore the system's functional stability is also obtained.

Using the methods of qualitative theory for differential equation systems with impulsive effects, a framework has been developed for determining strategies to minimize the impact of risk factors on the operation of a sensor network and to ensure its functional stability. An estimate of the functional stability reserve has been obtained for systems that admit an asymptotically stable impulsive periodic solution.

Future research may extend the proposed framework by incorporating spatially distributed models that account for network topology and the geographic heterogeneity of sensor deployment. The inclusion of stochastic effects and time-varying parameters would allow a more realistic representation of uncertainty in node failure, communication disruption,

and recovery processes. In addition, a dedicated investigation of the practical implementation aspects of the three recovery strategies considered in this work – constant monitoring, impulsive recovery, and periodic recovery – would be of particular interest, including their applicability, limitations, and performance trade-offs under realistic operational constraints. Finally, the integration of adaptive control mechanisms and learning-based strategies into the SIR-based framework presents a promising direction for developing autonomous and self-organizing sensor networks capable of dynamically optimizing their resilience under evolving operational conditions.

References

- [1] Azarov, O. (2017). AD systems for processing of low frequency signals based on self calibrate ADC and DAC with weight redundancy. *Przegląd Elektrotechniczny*, 1(5), 127–130. <https://doi.org/10.15199/48.2017.05.26>
- [2] Barabash, O., Musienko, A., Makarchuk, A., & Korotin, S. (2025). Method for Calculating the Sufficiency Criterion of Diagnostic Information for Executing the Self-Diagnosis Algorithm in Multi-Machine Information Systems. *Advanced Information Systems*, 9(2), 51–57. <https://doi.org/10.20998/2522-9052.2025.2.07>
- [3] Barabash, O., Svyanchuk, O., Salanda, I., Mashkov, V., & Myroniuk, M. (2024). Ensuring the functional stability of the information system of the power plant on the basis of monitoring the parameters of the working condition of computer devices. *Advanced Information Systems*, 8(2), 107–117. <https://doi.org/10.20998/2522-9052.2024.2.12>
- [4] Barabash, O. V., Musienko, A. P., & Sobchuk, V. V. (2022). Basics of ensuring the functional stability of information systems of enterprises under the influence of destabilizing factors: Monograph. Millennium, Kyiv.
- [5] Bryhynets, A., Klymenko, Y., Haidur, H., Gakhov, S., & Marchenko, V. (2025). Random Forest Approach for PDF Malware Detection. *Baltic Journal of Modern Computing*, 13(3). <https://doi.org/10.22364/bjmc.2025.13.3.08>
- [6] d'Onofrio, A. (2002). Pulse vaccination strategy in the sir epidemic model: Global asymptotic stable eradication in presence of vaccine failures. *Mathematical and Computer Modelling*, 36(4–5), 473–489. [https://doi.org/10.1016/S0895-7177\(02\)00177-2](https://doi.org/10.1016/S0895-7177(02)00177-2)
- [7] Dovzhenko, N., Barabash, O., Ausheva, N., Ivanichenko, Y., & Obushnyi, S. (2023). Comprehensive analysis of efficiency and security challenges in sensor network routing. *Cybersecurity Providing in Information and Telecommunication Systems II*, 3550, 275–280. <https://ceur-ws.org/Vol-3550/short12.pdf>
- [8] Dovzhenko, N., Barabash, O., Musienko, A., Ivanichenko, Y., & Krashenninik, I. (2024). Enhancing Sensor Network Efficiency Through Optimized Flooding Mechanism. *CEUR Workshop Proceedings, Vol-3654: Proceedings of the Workshop Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2024)*, 465–470. <https://doi.org/10.55056/ceur-ws.org/Vol-3654/short15.pdf>
- [9] Feketa, P., Klinshov, V., & Lücken, L. (2021). A survey on the modeling of hybrid behaviors: How to account for impulsive jumps properly. *Communications in Nonlinear Science and Numerical Simulation*, 103, 105955. <https://doi.org/10.1016/j.cnsns.2021.105955>
- [10] Hethcote, H. W. (1989). Three Basic Epidemiological Models. In S. A. Levin, T. G. Hallam, & L. J. Gross (Eds), *Applied Mathematical Ecology* (Vol. 18, pp. 119–144). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-61317-3_5
- [11] Jiao, J., Cai, S., & Li, L. (2016). Impulsive vaccination and dispersal on dynamics of an SIR epidemic model with restricting infected individuals boarding transports. *Physica A: Statistical Mechanics and Its Applications*, 449, 145–159. <https://doi.org/10.1016/j.physa.2015.10.055>
- [12] Kermack, W. O., & McKendrick, A. G. (1927). A contribution to the mathematical theory of epidemics. *Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character*, 115(772), 700–721. <https://doi.org/10.1098/rspa.1927.0118>
- [13] Makarchuk, A., Kal'chuk, I., Kharkevych, Y., & Voloshyna, T. (2020). Usage of Fourier Transformation in Theoretical Studying of Signals in Data Transmission. 2020 *IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT)*, 192–195. <https://doi.org/10.1109/ATIT50783.2020.9349308>
- [14] Rodrigues, H. S. (2016). Application of SIR epidemiological model: New trends. <https://doi.org/10.48550/ARXIV.1611.02565>
- [15] Semenova, O. O., Semenov, A. O., Bisikalo, O. V., Kucheruk, V. Yu., Kulakov, P. I., Romaniuk, R., Komada, P., & Nursetova, K. (2019). Applying artificial intelligence for cellular networks optimization. In R. S. Romaniuk & M. Linczuk (Eds), *Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2019* (p. 146). SPIE. <https://doi.org/10.1117/12.2536857>
- [16] Shuvatov, T., Suleimenov, B., & Komada, P. (2012). Gas turbine fault diagnostic system based on fuzzy logic. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska*, 2(3), 40–42.
- [17] Stone, L., Shulgin, B., & Agur, Z. (2000). Theoretical examination of the pulse vaccination policy in the SIR epidemic model. *Mathematical and Computer Modelling*, 31(4–5), 207–215. [https://doi.org/10.1016/S0895-7177\(00\)00040-6](https://doi.org/10.1016/S0895-7177(00)00040-6)
- [18] Sun, N., Shi, S., & Li, W. (2020). Singular renormalization group approach to SIS problems. *Discrete and Continuous Dynamical Systems - B*, 25(9), 3577–3596. <https://doi.org/10.3934/dcdsb.2020073>
- [19] Tanasiichuk, S. (2026). Hybrid method of adaptive control of variable mode of unmanned aerial vehicles with intelligent online compensation of disturbances. *Computer Systems and Information Technologies*, (1), 205–214. <https://doi.org/10.31891/csit-2026-1-19>
- [20] Wang, J. (2021). Dynamics and bifurcation analysis of a state-dependent impulsive SIS model. *Advances in Difference Equations*, 2021(1), 287. <https://doi.org/10.1186/s13662-021-03436-3>

D.Sc. Valentyn Sobchuk

e-mail: sobchuk@knu.ua

Professor of the Department of Integral and Differential Equations.

Research interests: information technologies, functional stability of complex technical systems, stability theory, mathematical modelling.

<https://orcid.org/0000-0002-4002-8206>

D.Sc. Yurii Kravchenko

e-mail: yurii.kravchenko@knu.ua

Professor, Head of the Networking and Internet Technologies Department.

Research interests: telecommunication systems, functional stability of complex technical systems, artificial intelligence.

<https://orcid.org/0000-0002-0281-4396>

B.Sc. Mykhaylo Sharapov

e-mail: mykhaylo.sharapov@gmail.com

Postgraduate student of the Department of Information Systems and Technology.

Interested in: deep learning, functional stability of wireless sensor networks.

<https://orcid.org/0009-0007-8225-0677>

D.Sc. Oleksandr Laptiev

e-mail: alaptiev64@ukr.net

Assistant professor of the Department of Cyber Security and Information Protection.

Research interests: information protection/cyber security, technical information security systems.

<https://orcid.org/0000-0002-4194-402X>

Ph.D. Andrii Sobchuk

e-mail: anri.sobchuk@gmail.com

Associate professor of the Educational-scientific Institute of Cyber Security and Information Protection, Department of Cybernetic Security Systems and Technologies.

Research interests: functional stability of complex technical systems, protection of information resources of enterprises, computer networks, industrial informatics.

<https://orcid.org/0000-0003-3250-3799>

