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

Sobchuk Valentyn[1], **Kravchenko Yurii**[1], **Sharapov Mykhaylo**[1], **Laptiev Oleksandr**[1], **Sobchuk Andrii**[2]
[1]*Taras Shevchenko National University of Kyiv, Kyiv,* [2]*State University of Information and Communication Technologies, Kyiv*

Abstract: *Wireless sensor networks are considered a promising technological approach for continuous monitoring, risk detection, and adaptive response in large-scale, hazardous, and dynamically changing environments, including border surveillance and disaster-zone monitoring. In disaster-zone applications, they offer substantial potential to support life-saving early warning and emergency response. The operation of sensor networks in the areas of monitoring is subject to numerous destabilizing factors, which necessitates the search for ways to enhance their functional stability. Understanding the behavior of a sensor network under the influence of adverse factors is critically important for timely forecasting of its degradation and preventing critical failures through the implementation of adaptive mechanisms and strategies to improve functional stability. Despite the significant number of studies in the field of strategies for ensuring the functional stability of sensor networks, the dependence of risk growth on time and the dynamics of network operation under hazardous conditions remain insufficiently explored. This work applies the framework of the qualitative theory of differential equations to describe and characterize the state of the system under risk exposure. 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. Conditions for maintaining the operational state of the network are determined through the application of various strategies to minimize the number of compromised devices, and the effect of these strategies is analyzed using phase plane methods. The dependence of network stability on the model parameters describing the rates of device failure and replacement/recovery is established. A model for determining the time required to restore the operational state of the system is obtained. A mathematical framework is developed to define strategies for minimizing the impact of risk factors on the functioning of the sensor network, based on methods from the qualitative theory of differential equation systems with impulsive action.*

Keywords: sensor network, functional stability strategy, SIR model, system of differential equations with impulsive action.

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 [2, 6].

Monitoring of borders and disaster zones is crucial for ensuring public safety, protecting critical infrastructure, and enabling timely responses to emerging threats. In border areas, continuous surveillance helps prevent unauthorized crossings, smuggling, and other illegal activities, contributing to national security and law enforcement efficiency. In disaster zones, real-time monitoring allows for rapid detection of hazards such as floods, wildfires, earthquakes, or industrial accidents, facilitating early warning and rescue interventions. Population growth, technological development, and geopolitical instability are creating novel challenges for both border and disaster-zone monitoring. These developments generate unprecedented demands for rapid, large-scale surveillance and timely early-warning systems. Wireless sensor networks have a proven capacity to carry out essential monitoring tasks across extensive areas exposed to hazardous conditions. [12].

Solving these tasks enables the formation of 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 affecting risk factors. In disaster-zone applications, WSN potential to support life-saving early warning and emergency response is crucial.

Integrated systems for terrain monitoring and autonomous navigation are capable of fulfilling a broad spectrum of functional objectives. However, such systems are inevitably subject to destabilizing factors, including environmental hazards and unexpected disruptions that can impair individual network components or compromise the overall operation of the system.

To mitigate potential adverse impacts, such systems must exhibit adaptive behavior. This adaptability enables the preservation of core functionality even under conditions of partial destruction or intentional interference. System adaptability involves selecting and executing appropriate strategies to maintain or restore core functionality while the system is continuously exposed to harmful factors.

Accordingly, the study of the behavioral 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.

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 [4], 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 [3]. 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 analog-to-digital network based on current converters with weight redundancy is presented in [1]. In [18], anomaly detection in sensor networks using Fourier transformations is examined. The work in [8] investigates the application of machine learning methods – specifically, support vector machines 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 [17]. More in-depth analyses of corresponding results for complex sensor networks can be found in [16, 19]. Methods for ensuring the stable operation of a wireless wide area network using a neuro-fuzzy controller are discussed in [14]. A method for parametric diagnostics of the functional stability of a mechanical system employing fuzzy logic is proposed in [15].

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 [9, 11] makes

it possible to investigate the state of a complex system in dynamics. In [13], 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 [5, 10, 20 - 22] analyze the impact and effectiveness of various vaccination strategies and approaches. In [7], it is demonstrated that the theory of differential equations with impulsive action can be employed for the purposes of formalizing and analyzing dynamics.

2. Representing the Stability of a Sensor Network Using the SIR Model

The issue of ensuring the functional stability of complex information systems supporting the protection of population and territory has become particularly relevant. Wireless sensor networks deployed for border and disaster-zone monitoring need to cover large and varied terrains, integrate fixed and mobile nodes, and accommodate both high-resolution monitoring and low-power long-duration operation under dynamic environmental conditions. They comprise a diverse mix of sensor types, communication protocols, and energy sources, and can be regarded as a complex heterogeneous network continuously subjected to a variety of external and internal destabilizing factors. 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 analyze the principal risks to which wireless sensor network devices are exposed in border surveillance and disaster-zone monitoring environments. 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 in Border and Disaster Monitoring

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 modeling of evolutionary processes for ensuring the functional stability of a complex wireless sensor network for monitoring and navigation across the zone of the border and disaster monitoring, 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 [9, 11, 13].

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, 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:

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

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 behavior. 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 behavior 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 behavior 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 behavior 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).

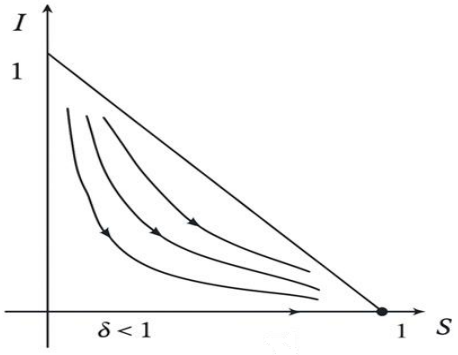
Under these circumstances, the qualitative behavior of system (1) is determined by the value of the parameter δ. Theorem holds.

Theorem 1. [5] For $\forall\delta > 0$ the domain $\mathcal{D}$ is invariant, i.e. $\forall(\mathrm{S_0}, \mathrm{I_o}) \in \mathcal{D}$ the solution of system (1) (S(t), I(t)) with initial conditions $\mathrm{S}(0) = \mathrm{S_0}$, $\mathrm{I}(0) = \mathrm{I_0}$ remains in $\mathcal{D}$, $\forall\mathrm{t} \geq 0$, that is, $\big(\mathrm{S(t)}, \mathrm{I(t)}\big) \in \mathcal{D}$, $\forall\mathrm{t} \geq 0$.

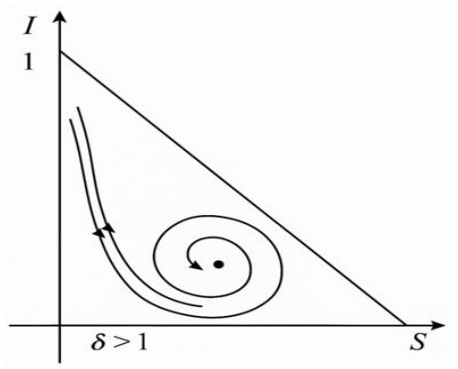
For $\forall\delta > 0$, system (1) has no closed trajectories in $\mathcal{D}$.

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

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



a)



b)

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 $\mathcal{D}$ llows us to conclude that such behavior 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 newborns 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:

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

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

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

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

Theorem 2. [10] For $\forall\mathrm{p} \in (0,1)$, the domain $\mathcal{D}$ is invariant in system (2). Within the domain $\mathcal{D}$ there are no closed trajectories of system (2).

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

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

Thus, stability - and, consequently, the resilience of the network for $\mathrm{p} > \mathrm{p}_*$ is ensured at the point $\big(\hat{\mathrm{S}}_0^*, \hat{\mathrm{I}}_\mathrm{o}^*\big)$, while for $\mathrm{p} < \mathrm{p}_*$ it is realized at the point $\big(\hat{\mathrm{S}}_1^*, \hat{\mathrm{I}}_1^*\big)$. However, in the situation where $\mathrm{p} > \mathrm{p}_*$ in the neighborhood of $\big(\hat{\mathrm{S}}_1^*, \hat{\mathrm{I}}_1^*\big)$ and where $\mathrm{p} < \mathrm{p}_*$ in the neighborhood of $\big(\hat{\mathrm{S}}_0^*, \hat{\mathrm{I}}_\mathrm{o}^*\big)$ 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 modeling 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:

$$\begin{cases} \dfrac{dS(t)}{dt} = -\lambda S(t)I(t) + \mu - \mu S(t), \quad t \neq t_n, \\ \dfrac{dI(t)}{dt} = \lambda S(t)I(t) - \gamma I(t) - \mu I(t), \quad t \neq t_n, \end{cases} \tag{3}$$

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

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

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

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

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

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

This solution is asymptotically stable under the condition

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

Corollary. The functional stability reserve of a complex wireless sensor network for monitoring and navigation 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 $t \to \infty$ is shown in Fig. 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.

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

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

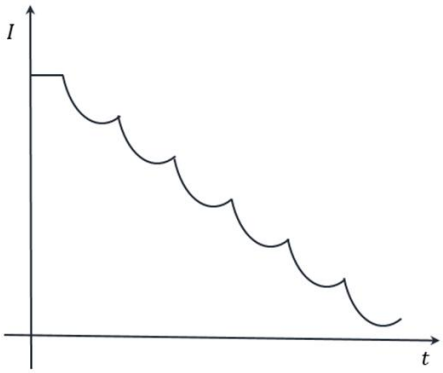


Fig. 2. Illustration of the behavior of $I(t)$, $I(0) = I_0 \in (0,1)$ as $t \to \infty$.

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

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

then the condition $I(t) \to 0$, $t \to \infty$ 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: $t_n = nT$, $n = 0,1,\ldots$.

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

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

$$\overline{\lim_{\tau\to\infty}} \frac{N(t, t+\tau)}{\tau} < \infty,$$

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 behavior 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.

3. Conclusion

Wireless sensor networks employed for border patrolling and disaster-zone monitoring have great potential for providing large-scale, continuous situational awareness and early warning, which constitutes an integral component of modern risk response capability and simultaneously contributes to enhancing national security.

To ensure the functional stability of complex information and communication systems for monitoring and navigation across the area of border or disaster monitoring, 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 work presents methods that enable the maintenance of functional stability of sensor networks under the influence of internal and external adverse factors. The models and behaviors of complex information systems are described by systems of differential equations with impulsive effects and analyzed using the methods of qualitative theory of differential equations. 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.

References

[1] Azarov, O. D., et al.: AD systems for processing of low frequency signals based on self calibrate ADC and DAC with weight redundancy. Przegląd Elektrotechniczny. 93(5), 2017, 125–128.

[2] Barabash O. et al.: Algorithms for synthesis of functionally stable wireless sensor network // Advanced Information Systems, 9(1), 2025, 70–79 [https://doi.org/10.20998/2522-9052.2025.1.08].

[3] Barabash, O., et al.: System Analysis and Method of Ensuring Functional Sustainability of the Information System of a Critical Infrastructure Object. In: Zgurovsky, M., Pankratova, N. (eds) System Analysis and Artificial Intelligence. Studies in Computational Intelligence, vol 1107. Springer, Cham 2023. [https://doi.org/10.1007/978-3-031-37450-0_11]
[4] Barabash O.V., Musienko A.P., & Sobchuk V.V.: Basics of ensuring the functional stability of information systems of enterprises under the influence of destabilizing factors: monograph. Millennium, Kyiv 2022.
[5] D'Onofrio A.: Pulse Vaccination Strategy in the SIR Epidemic Model: Global Asymptotic Stable Eradication in Presence of Vaccine Failures. Mathematical and Computer Modelling. 36, 2002, 473–489.
[6] Dovzhenko N., et al.: Enhancing sensor network efficiency through optimized flooding mechanism. Cybersecurity Providing in Information and Telecommunication Systems - CPITS-2024, 2024, 465–470.
[7] Feketa P., Klinshov V., & Lücken L.: A survey on the modeling of hybrid behaviors: How to account for impulsive jumps properly. Commun Nonlinear Sci Numer Simulat, 103, 2021, 105955 [https://doi.org/10.1016/j.cnsns.2021.105955].
[8] Haidur, H., Gakhov, S., & Hamza, D.: Using support vectors to build a rule-based system for detecting malicious processes in an organisation's network traffic. Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska, 14(4), 2024, 90–96.
[9] Hethcote, H. W.: Three Basic Epidemiological Models. Applied Mathematical Ecology. Springer, Berlin-Heidelberg 1989.
[10] Jiao J., Cai S., & Li L.: Impulsive vaccination and dispersal on dynamics of an SIR epidemic model with restricting infected individuals boarding transports. Physica A. 449, 2015, 145–159.
[11] Kermack, W. O., McKendrick, A. G.: 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), 1927, 700–721.
[12] Kravchenko Yu., Dakhno, N.: Strategy of intelligent control of the flexible structure of a complex system of autonomous navigation in the format of GPS-signals and sensor monitoring of the combat line with UAVs. Air Force of Ukraine, 6(1), 2024, 5–13 [https://doi.org/10.33099/2786-7714-2024-1-6-5-13].
[13] Rodrigues H.S.: Application of SIR epidemiological model: new trends. International journal of applied mathematics and informatics. 10, 2016, 92–97.
[14] Semenova, O. O., et al.: Applying artificial intelligence for cellular networks optimization. Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments - SPIE. 2019. Vol. 11176.
[15] Shuvatov, T., Suleimenov, B. & Komada P.: Gas turbine fault diagnostic system based on fuzzy logic. Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska. 2(3), 2012, 40–42.
[16] Sobchuk A.V., et al.: Functionally sustainable wireless sensor network technologies aspects analysis. Science and Education a New Dimension. VII (193), 2019, 46–48.
[17] Sobchuk, V., Barabash, O., & Musienko, A.: The influence of the method of adaptive self-diagnosis on the process of preventing the consequences of failures of modules of the information system of the enterprise. Collection of scientific works of the Military Institute of Taras Shevchenko Kyiv National University, 70, 2021, 77–88 [https://doi.org/10.17721/2519-481X/2021/70-08].
[18] Sobchuk, V., et al.: A modified method of spectral analysis of radio signals using the operator approach for the Fourier transform. Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska, 14(2), 2024, 56–61.
[19] Sobchuk V.V., Dovzhenko N.M., & Koval M.O.: Mathematical model of multi-criteria optimization of service quality of sensor networks using the principle of fairness. Telecommunications and Information Technologies. 64(3), 2019, 90–97.
[20] Stone L., Shulgin B., & Agur Z.: Theoretical Examination of the Pulse Vaccination Policy in the SIR Epidemic Model. Mathematical and Computer Modelling. 31, 2000, 207–215.
[21] Sun N., Shi Sh., & Li W.: Singular renormalization group approach to SIS problems. Discrete and continuous dynamical systems Series B. 25(9), 2020, 3577–3596.
[22] Wang J.: Dynamics and bifurcation analysis of a state-dependent impulsive SIS model. Advances in Difference Equations. 287, 2021, 1–19 [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.

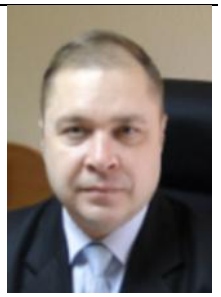
https://orcid.org/0000-0002-4002-8206

D.Sc. Kravchenko Yurii
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



Sharapov Mykhaylo
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. Laptiev Oleksandr
e-mail: alaptev64@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