UDC 004.056:51-74

Reference functions of cyber incidents displaying in the media space

D. V. Lande[1], O. M. Novikov[1], I. V. Stopochkina[1]

[1] *National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Educational and Research Institute of Physics and Technology*

Abstract

The principles of cyber attacks detection that based on media content are described. Proposed methods are suitable for description of the general trends in the dynamics of information flows concerning cyber incidents. A generalized diagram of cyber attacks stages displaying in the media space is proposed. On the basis of the diagram the basic wavelet functions are selected, which can be considered as a reference for detecting cyber incidents. The proposed wavelets are low-order derivatives of Gaussian function (Wave, «Mexican Hat» and Morlaix wavelets). Retrospective analysis of already implemented information operations is a reliable way to verify them. The problem of forecasting is partly solved by probabilistic estimates in accordance with the type of reference functions.

Keywords: Media space, cyber incident, reference function, information flows, cyber attack detection, wavelet transform

Introduction

Numerous cyber incidents that are occurring at this time, apparently, are reflected in the modern media space of the Internet (on websites, social networks, video hosting, etc.). Very often cyber attacks can be a part of information operations, the reflection of which in the media space is widely studied and presented in numerous publications [1, 2, 3]. Manifestations of cyber incidents in the media space, in the dynamics of information flows, may have their own characteristics, however, the study of the behavior of the relevant information flows in the media space is still quite limited. Detection of templates, reference functions of cyber attacks in the information space, such as templates of cyber incidents in networks [4] allows to detect cyber attacks in the archives of information messages, detect current cyber attacks, and in some cases, to predict the development of cyber incidents. The main idea of the study described in this article is as follows:

1) Templates (reference functions) for displaying cyber attacks in the media space are calculated on the basis of social media monitoring information. It is assumed that the media space, in particular, websites – is a reflection of public opinion.
2) It is assumed that two main types of reports on cyber incidents are published on social media: A) reports on new cyber incidents, cyberattacks (type A reports); B) previous reports of cyber incidents, official reports and comments on these events (type B reports).
3) The reference functions for displaying cyber attacks in the media space should correspond to the time and level of the relationship between the volume of type A publications and the corresponding type B messages. This relationship can, in particular, be calculated as a correlation between relevant message flows.
4) The overall flow of cyber incident messages in cyberattacks is a technically difficult-to-separate mix of type A and B messages. The relationship between type A and B messages can be displayed as autocorrelation for the overall cybersecurity information flow cyber attacks.

Traditional analysis of information flows dynamics

The world community is increasingly using information from open sources to solve a wide range of problems. Many modern information and analytical systems include tools for displaying statistics on the occurrence of concepts that meet user requirements. In particular, the authors used the statistics subsystem within the InfoStream content monitoring system of the web space [5], which implements this functionality.

When studying such trends in cyber incidents, time series are considered to be series in terms of the number of thematic publications for a certain period of time (most often – per day) that correspond to these cyber incidents (more precisely, queries related to them).

The role of OSINT (Open Source Intelligence) [6] in cyber incidents detection is determined by a number of aspects, including the algorithm efficiency, volume, quality, clarity, ease of use, cost of actions and more. The following factors affect the process of planning and preparing for OSINT:

- Effective information support. Most of the necessary information on cyber incidents is obtained from open sources.
- Availability, depth and scope of publicly available information allows to find the necessary information without the use of specialized tools.
- Simplification of data collection processes.
- Depth of data analysis. OSINT allows you to analyze all publicly available information.
- Efficiency. A sharp reduction in access time.

- Volume. Ability to monitor mass sources of information in order to find interesting content, people and events.
- Quality. Information is devoid of subjectivity.
- Ease of use. It is possible to conduct a comprehensive investigation based on data from the Internet.
- Cost. The price of data extraction is minimal, determined only by the cost of the service used.

Therefore, to identify trends, information flows corresponding to cyber incidents are studied – thematic information flows. Numerous scientific works [7, 8, 9] are devoted to the study of the dynamics of information flows, where it is shown that in typical situations the dynamics of information story dissemination is characterized by the nature of «burst», waves with a clear period of growth and subsequent decline. The trends of messages corresponding to the stages of the information operation are shown in [10], shown on Fig. 1. Analysts should focus on the following models, for example, if monitoring allows to determine the phases: «background» – «calm» – «training» – «calm» – «attack». The first three components are likely to predict future events.

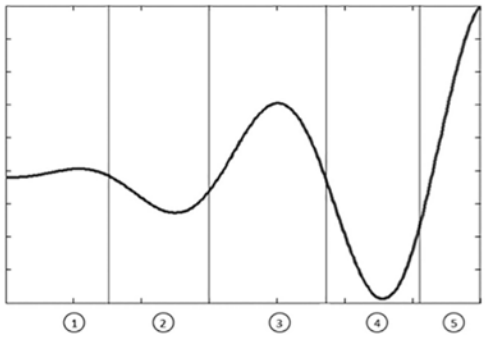


Fig. 1. Dynamics of the number of thematic messages during the information operation: 1 – background; 2 – calm; 3 – training; 4 – calm; 5 – attack/growth

It should be noted that such dynamics of the number of thematic messages during information operations is well described by the known equation of propagation of electromagnetic waves:

$$y = A + Bx \sin x, \qquad (1)$$

where x — time, A and B — empirically determined constants.

The general flow of reports of cyber incidents

To conduct the study at the first stage with the help of the InfoStream content monitoring system, the dynamics of the number of thematic reports on cybersecurity was obtained daily for 6 years: from 2016 to 2021. The thematic flow was determined by the query information retrieval language of this system (in ukrainian):

```
кібератак|кіберпреступ|кібератак|
|кіберзлочин|(хакер@атак)
```

In total, more than 600,000 thematic reports were taken into account. The system issued data related to the number of messages for each day of the observation period. Relevant data were aggregated, combined into a single time series (Fig. 2).

Content analysis

As a result of automatic information-analytical processing, which was carried out using the InfoStream system, the main story chains were obtained, which correspond to the dates with the highest number of messages for this query in 2020 (Fig. 3, 4). Obviously, different types of messages related to different cyber incidents are mixed up in the general information flow. Correlation analysis, the results of which are given below, should help to identify the features of their distribution.

On Fig. 5, 6, 7, 8 the diagrams of Dynamics of messages on the topics of individual cyber incidents are presented («Cyberattack on the Colonial Pipeline» and «Cyberattack on the water supply system of Florida state (USA))», as well as fragments of main story chains selections on these topics.

Correlation analysis

Correlation analysis, in particular the properties of autocorrelations, is used to identify internal dependencies inside of the information flow.

Let X_t – is the message sequence number that were received, e.g., per day t, $t = 1, ..., N$, then the autocorrelation function for series is defined as:

$$F(k) = \frac{1}{N-k} \sum_{i=1}^{N-k} (X_{k+t} - m)(X_t - m), \qquad (2)$$

where m – the average of the series X.

Autocorrelation function of real cybernetic operation

In the environment of the Matlab system, the autocorrelation of the time series was calculated using the xcorr function,and graphically presented on Fig. 9, where the abscissa is marked by the value of autocorrelation, and the ordinate – time offsets (per day). Shown on Fig. 9 the autocorrelation function has a complex nonlinear structure, the objectives of the study obviously correspond to the values of local extrema. These data can be used in the formation of the pattern of cyberactivity.

Some cyber incidents are characterized by an autocorrelation function, similar to the function of the general information flow (Fig. 10), which gives grounds to determine the features of cyber incidents represented by the media space information.

Comparison with other thematic streams

According to the proposed methodology on the same basis, at the same time, autocorrelations were calculated for other information flows related to terrorism (Fig. 11a) and ecology (Fig. 11b). Comparison of these results with the values of the autocorrelation function for the subject of cyberattacks confirms the possibility

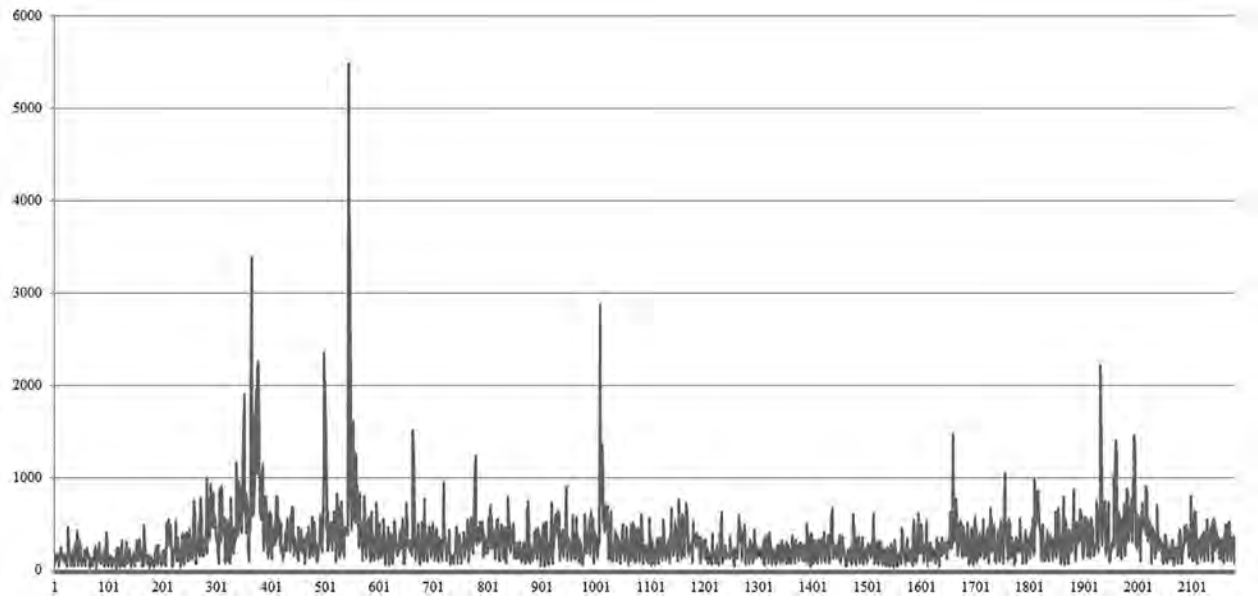


Fig. 2. Aggregate time series (horizontal axis – serial number of the day, vertical axis – the number of thematic messages)

Fig. 3. The main thematic stories for December 14, 2020. Type A.

Fig. 4. The main thematic stories for February 20, 2020. Type B.

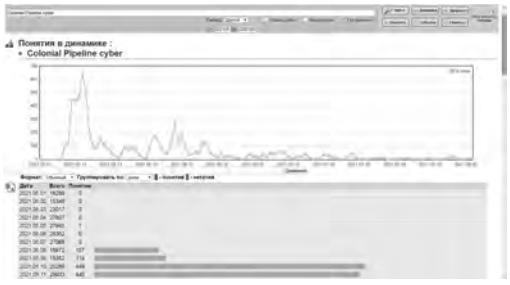


Fig. 5. Dynamics of messages on the topic «Cyberattack on the Colonial Pipeline»

of constructing a reference function as a template for cyberattacks based on the proposed approach.

General model of the cyber attacks representation process in the media space

The study of information flows of reports on cyber incidents, correlation analysis, allows to expand the model of information operations, described in [10] with additional stages, complicate the reference function with additional bursts corresponding to the stages of publishing the results of relevant cyberattacks investigations. The following generalized pattern chart corresponds to the number of cyberattack messages (vertical axis) over time. Fragments of this function may correspond to individual cyberattacks, which can be used as a template for detecting information operations by correlation analysis methods and other image recognition methods. Fig. 12 shows the following possible bursts on the timeline (diagram): 1st burst: preparation for a cyber incident, conditional «intelligence», 2nd burst: the actual cyberattack, 3rd burst: discussion stage, cyber attack investigation, 4th and further outbursts: mention of cyber attacks, for example, in the events of subsequent cyber incidents. It should be noted that real cyber incidents may not contain individual bursts, such as «intelligence» bursts, or «remembrance» bursts can be significantly distant in time.

Wavelet analysis of cyber attacks

To determine the degree of «proximity» of studied time series fragments to the diagram of cyber incident reflection in the media space on various scales, it is

Fig. 6. Fragment of the main plots selection on «Cyberattack on the Colonial Pipeline» topic

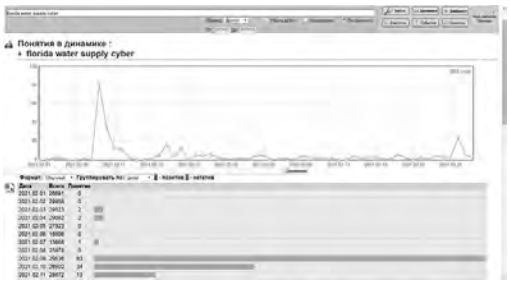


Fig. 7. Dynamics of messages on «Cyberattack on Florida Water Supply» topic

proposed to use «wavelet analysis», which has found application in natural science and sociology [11, 12]. The main idea of wavelet transform is that a nonstationary time series is divided into separate intervals (so-called «observation windows»), and each of them is used to calculate a value that shows the degree of closeness of the laws of the observed data with different shifts of a special function (wavelet) on different scales. The wavelet transform generates a set of coefficients that are functions of two variables: hours and frequencies, and therefore form a surface in three-dimensional space. Wavelet coefficients show how much the behavior of the process at each point is similar to the behavior of the wavelet at this scale. The main advantage of the wavelet transform is that the part selected from the time series is analyzed with the degree of detail that corresponds to its scale. The wavelet scaleogram shows all the characteristic features of the original series: the scale and intensity of periodic changes, the direction and significance of trends, the presence, location and duration of local features.

The wavelet transform, like the Fourier transform, can be considered in terms of correlation. In this case, the correlation of the original function with the wavelet function of different scales is considered. In order for such a procedure to always be possible and for the correlation coefficients to be informative, the wavelet function ψ_t should satisfy certain mathematical properties.

Function ψ_t is quadratically integrated ($\psi \in L^2(\mathbb{R})$ or, in other words, has finite energy

$$E = \int_{-\infty}^{\infty} |\psi(t)|^2 dt. \tag{3}$$

Denote $\hat{\psi}(\lambda)$ the Fourier transform of a function ψ_t,

$$\int_{-\infty}^{\infty} \frac{|\hat{\psi}(\lambda)|^2}{\lambda} d\lambda < \infty. \tag{4}$$

Enter the scale parameter s and location parameter l, then the converted version of the mother wavelet will be as follows

$$\psi_{s,l} = \frac{1}{\sqrt{|s|}} \psi\left(\frac{t-l}{s}\right). \tag{5}$$

Continuous wavelet transform function $x(t) \in L^2(\mathbb{R})$ is called an expression

$$W(s,l) = \frac{1}{\sqrt{|s|}} \int_{-\infty}^{\infty} x(t)\psi^*\left(\frac{t-l}{s}\right) dt = \\ = \int_{-\infty}^{\infty} x(t)\psi^*_{s,l}(t)dt, \tag{6}$$

where $l, s \in \mathbb{R}$, $s \neq 0$; ψ^* – complex conjugate function to ψ, values $\{W(s,l)\}_{l,s\in\mathbb{R}}$ are called wavelet transform coefficients.

From the given formula it is seen that the essence of such transformation consists in calculation of correlation coefficients of a special kind.

Based on the basic wavelet, a family of functions is built by stretching/compression and parallel transfer. This is necessary to explore different areas of the output signal and with varying degrees of detail.

With the help of continuous wavelet transform, the areas of the studied series that are most similar in shape to the wavelet are detected. The idea is to compare parts of a series with some pattern on different scales. The wavelet transform is the correlation between the original time series and the wavelet $\psi(t)$. Thus, the wavelet transform depends on the position of the wavelet on the time axis and its scale. The processes under consideration are clearly visible both on wavelet scaleograms and on the corresponding skeletons (graphs of extremum lines).

During the wavelet analysis, it was decided to use the wavelets Wave (Gaussian wave), MexH (Mexican hat) and Morlaix (all are the low-order derivatives of Gaussian function), as close in shape to the diagram shown on Fig. 13.

The resulting wavelet coefficients can be represented graphically by postponing the wavelet offset (time axis) and the scale (axis of scales) on one axis, and color the points of the resulting scheme depending on the size of the corresponding coefficients, the higher the coefficient, the brighter the colors).

These coefficients show how similar the behavior of the process at this point is to the wavelet at this scale. The closer analyzed dependence within a given point to the type of wavelet, the greater the absolute value of the corresponding coefficient. The application of these

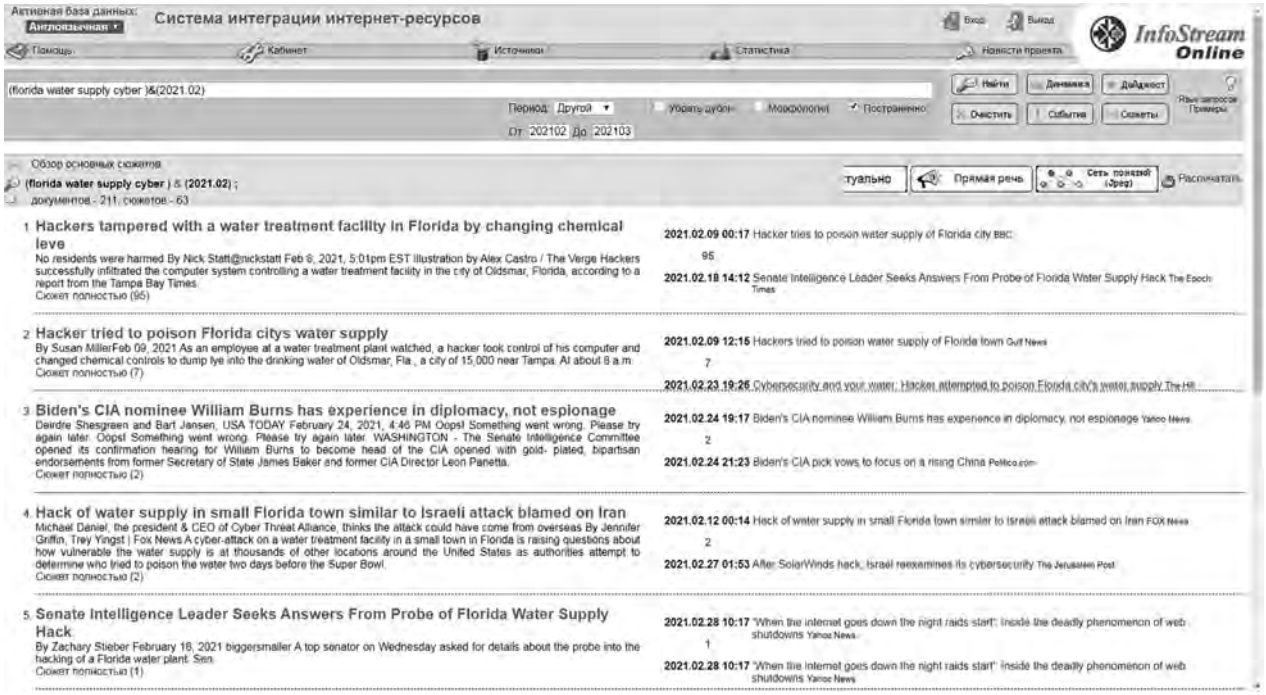


Fig. 8. Fragment of a main plots selection on «Cyberattack on Florida Water Supply» topic

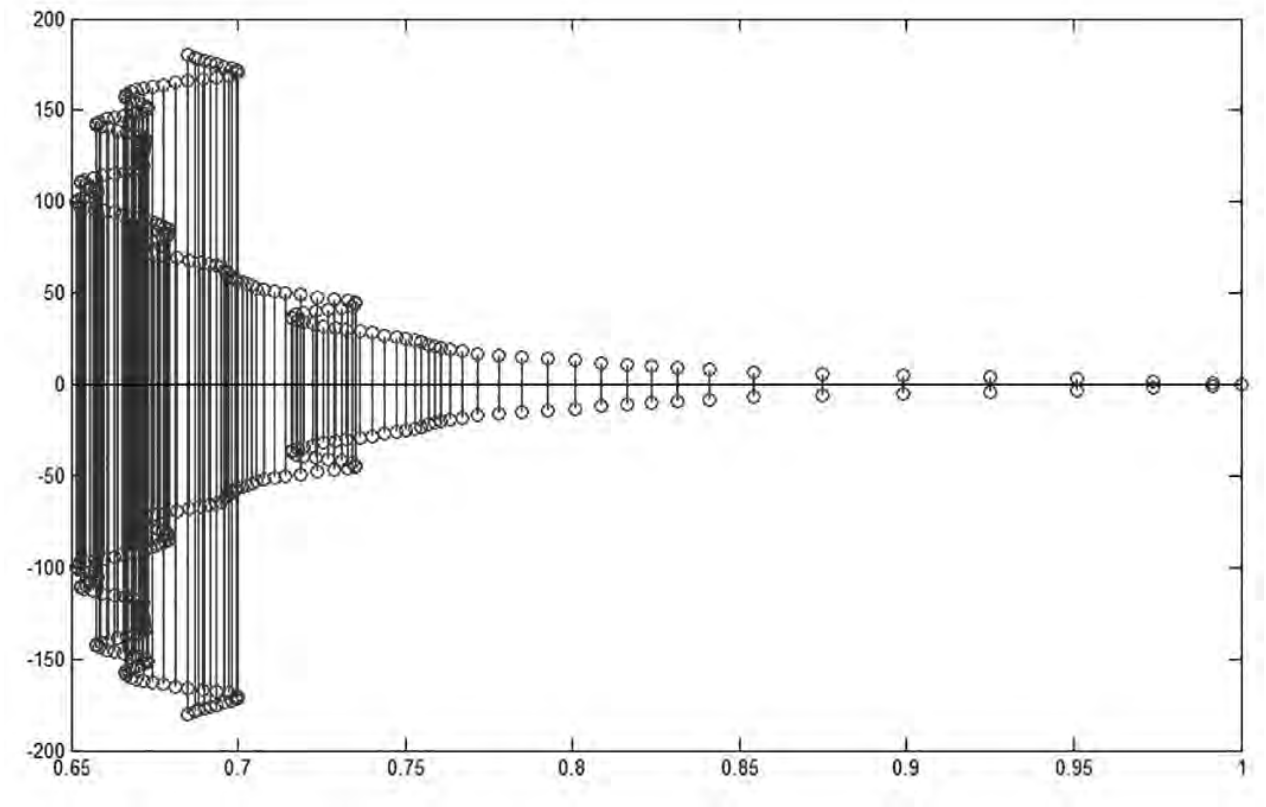


Fig. 9. Autocorrelation function that corresponds to the dynamics of the overall information flow on cybersecurity

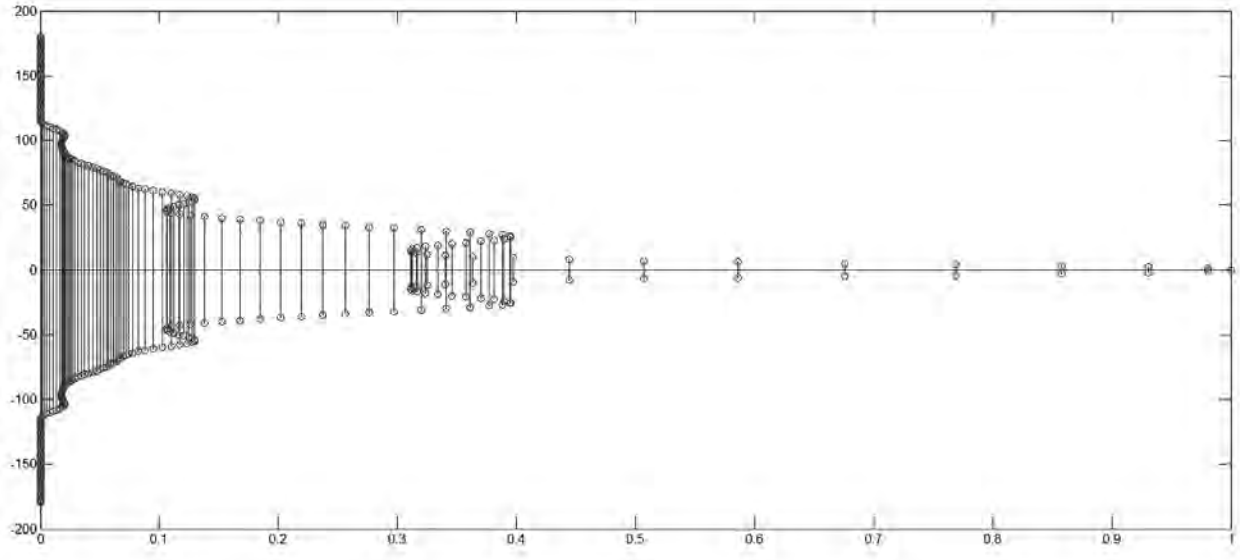
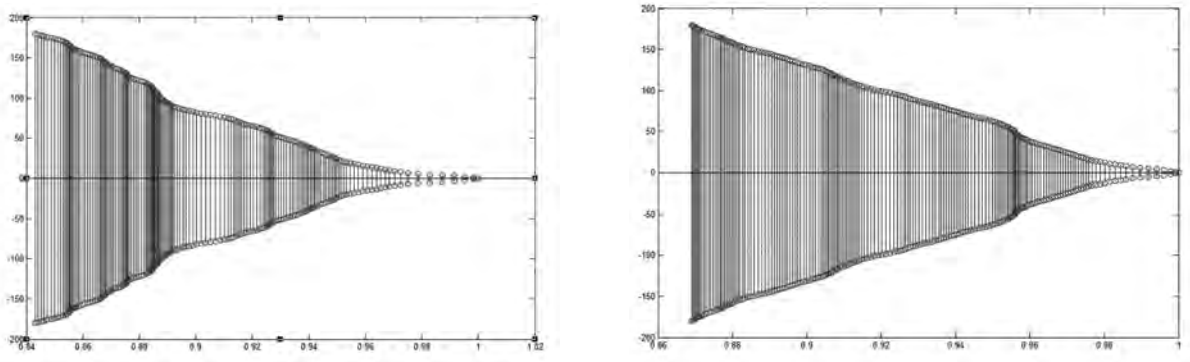


Fig. 10. Autocorrelation function corresponding to the dynamics of messages about cyber attack on the Colonial Pipeline



(a) (b)

Fig. 11. Autocorrelation function corresponding to the dynamics of reports on terrorism (a) and ecology (b)

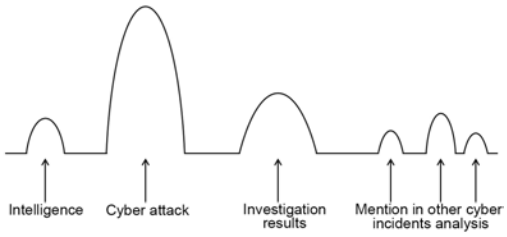


Fig. 12. Stages of displaying the information about cyber attacks

operations, taking into account the properties of the locality of the wavelet in the frequency-time domain, allows to analyze data at different scales and accurately determine the position of their features over time.

On the scaleograms you can see all the characteristics of the original series: the scale and intensity of periodic changes, the direction and significance of trends, the presence, location and duration of local features.

The following Fig. 14– 16 are the results of a rapid analysis of thematic information flows in response to the two cyber attacks on the Florida State Water System, the Colonial Pipeleine, and the 2016 General Cyber Incident Information Flow. 2021.

The scaleograms show that the complication of the wavelet (the first derivative of the Gaussian function, the second derivative, the third derivative), provides an increase in the level of detail from a generalized view - Wave wavelet to detailed - Morlaix wavelet. Obviously, the Morlaix wavelet (Fig. 13c) and the presented scaleograms supply a sufficient level of details.

However, the choice of templates as derivatives of the Gaussian function does not claim to be fully complete, it is not even limited to wavelets. Other approaches are possible. Wavelet as a function must have certain mathematical properties, in particular, rapidly decrease to zero at infinity. In some cases, it is useful to use a template that does not meet the wavelet requirements. To do this, instead of a wavelet transform, we can calculate the correlation between part of the time series and some pattern p [1]:

$$C(l,k) = \frac{\sum\limits_{i=1}^{k}(x_{l+i} - \overline{x})(p_i - \overline{p})}{\sqrt{\sum i = 1k(x_{l+i} - \overline{x})^2(p_i - \overline{p})}} \qquad (7)$$

The obtained coefficient $C(l,k)$ depends on the values $x_{l+1}, ..., x_{l+k}$. That is the parameter l corresponds to template offset, and parameter k in this case it is analogous to scale s, which was used during the wavelet transform.

Conclusions

Considered models and methods are suitable for describing general trends in the dynamics of information processes. Wavelets are considered as reference functions. We consider a derivatives of different orders from the Gaussian function (Wave, MexH and Morlaix wavelets), which correspond to the general diagram of cybernetic attacks in the media space proposed in the article. Retrospective analysis of already implemented information operations proved to be a reliable way to verify them. The problem of forecasting partly is solved by probabilistic estimates of the continuation of the proposed pattern. Obviously, more realistic models can be obtained taking into account an additional set of factors, most of which are reproduced over time. In addition to the dynamics of time series, it is necessary to analyze the content of information messages. Numerous parameters extracted from texts by the Text Mining methods, which can be used later in machine learning as parameters of the recognition system, must be taken into account.

(a) (b) (c)

Fig. 13. Examples of wavelets that can be used in the analysis of cyber attacks: (a) Gaussian wave (the first derivative of Gaussian function), (b) Mexican hat, (c) Morlaix's wavelet (real part)

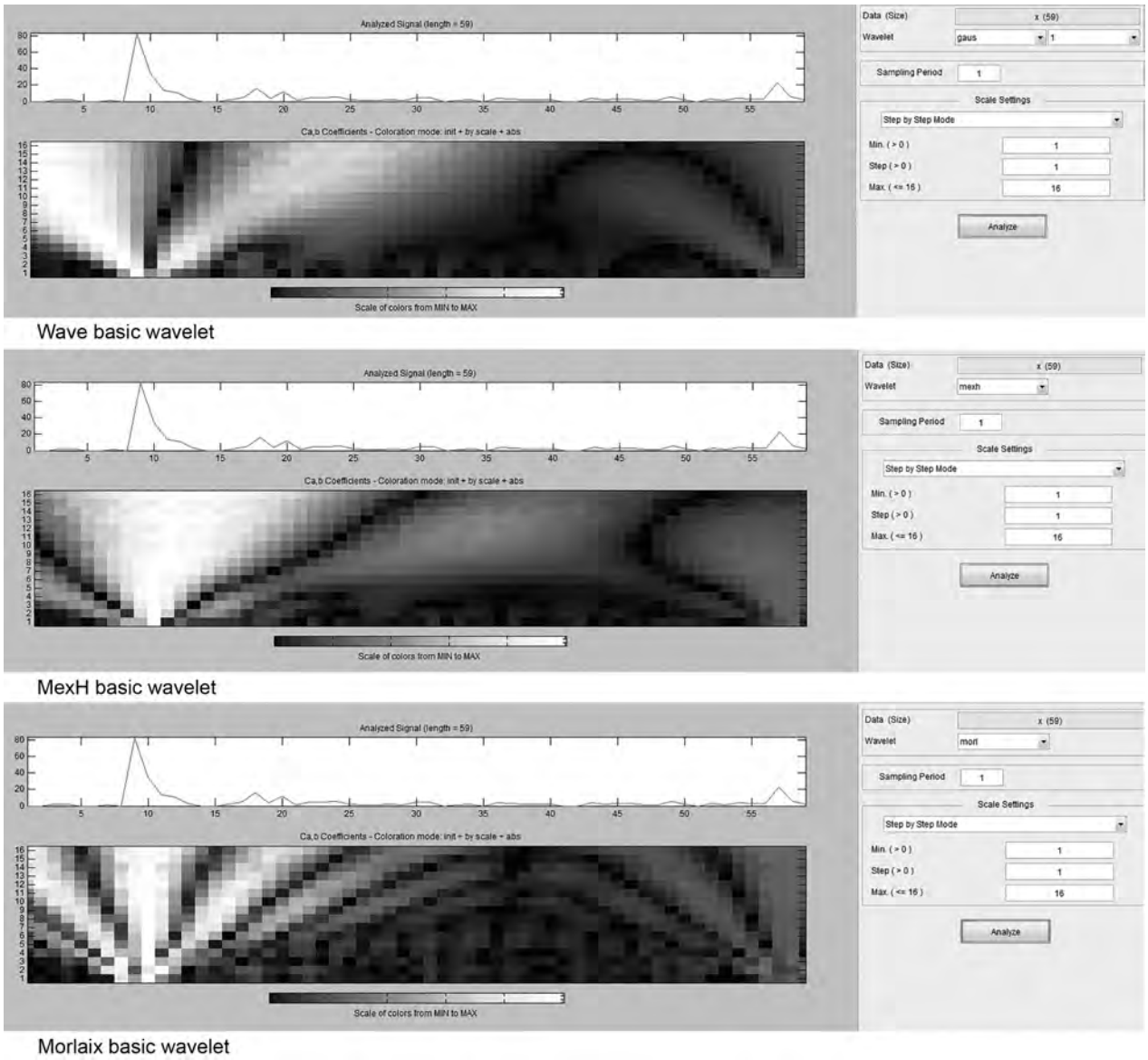


Fig. 14. Wavelet scaleogram of the time series corresponding to the cyber attack on the Florida water system

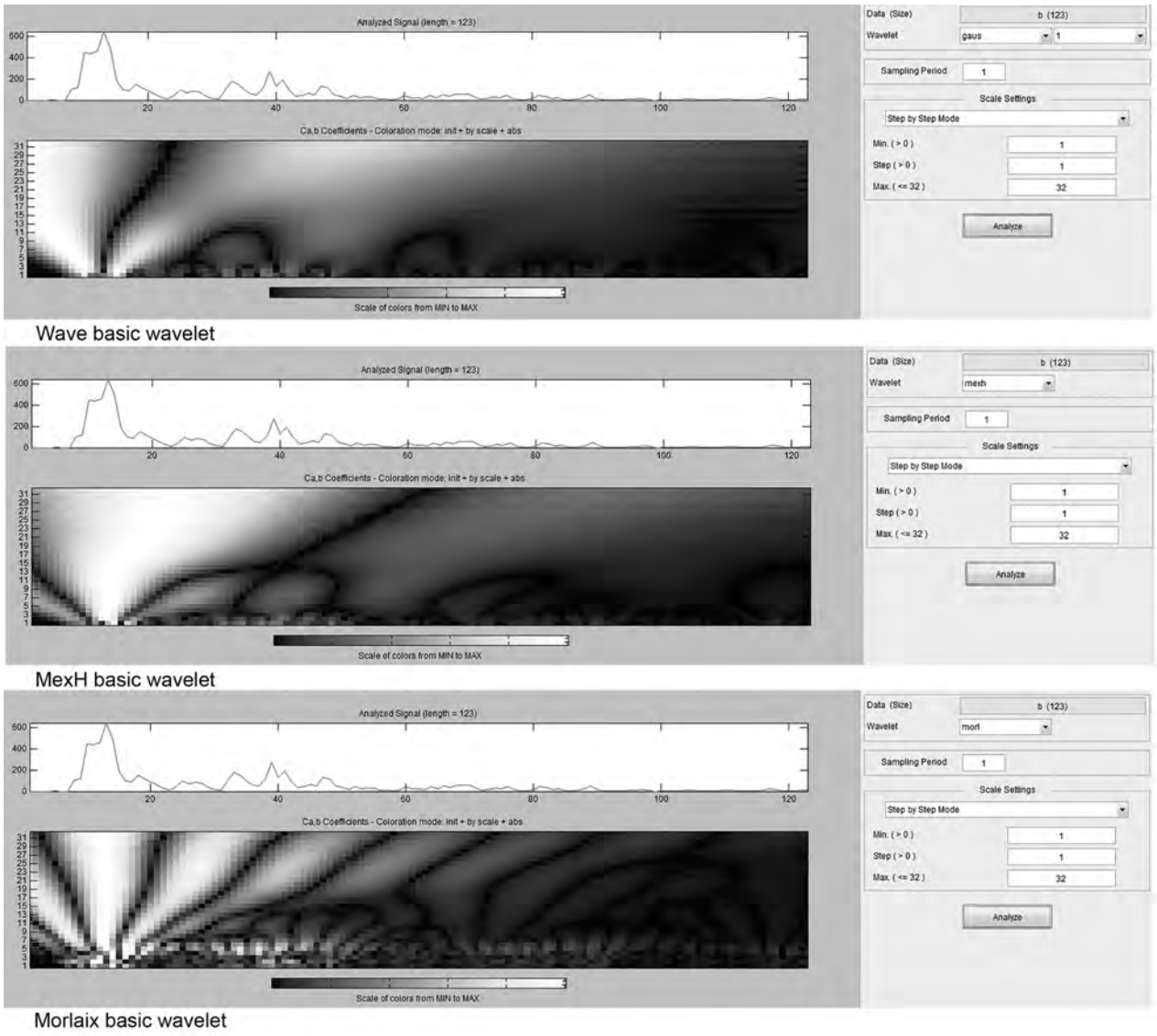


Fig. 15. Wavelet scaleograms of the time series corresponding to the cyber attack on the Colonial Pipeline

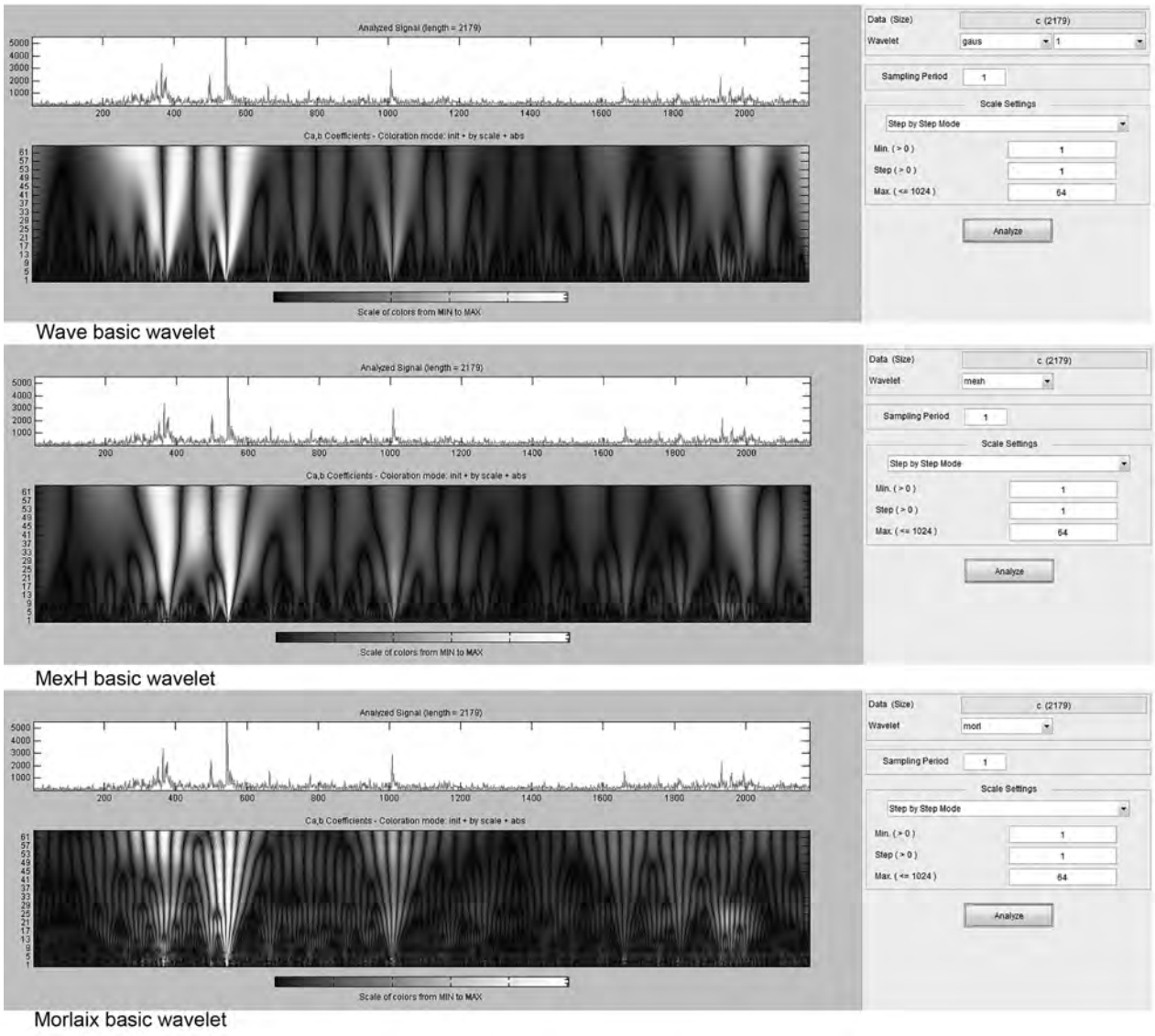


Fig. 16. Wavelet scaleograms of the time series, which correspond to the general information flow on cyber incidents topics for 2016–2021

References

[1] Information Operations Recognition. From Nonlinear Analysis to Decision-Making / A. Dodonov, D. Lande, V. Tsyganok et al. — LAP Lambert Academic Publishing, 2019. — ISBN: 6200276978.

[2] Starbird K., Arif A., Wilson T. Disinformation as Collaborative Work: Surfacing the Participatory Nature of Strategic Information Operations // Proceedings of the ACM on Human-Computer Interaction. — 2019. — 11. — Vol. 3, no. 127. — P. 1–26.

[3] Weedon J., Nulan W., Stamos A. Information Operations and Facebook. 2017 Facebook. — Access mode: `https://about.fb.com/br/wp-content/uploads/sites/3/2017/09/facebook-and-information-operations-v1.pdf`.

[4] Cybersecurity named entity recognition using multi-modal ensemble learning / F. Yi, B. Jiang, L. Wang, J. Wu. // IEEE Access. — 2020. — Vol. 8. — P. 63214 – 63224. — DOI: 10.1109/ACCESS.2020.2984582.

[5] InfoStream. Monitoring of news from the Internet: technology, system, service: scientific and methodical manual (in Russian) / A. N. Grigoriev, D. V. Lande, S. A. Borodenkov et al. — OOO «Start-98», Kyiv, 2007. — 40 p.

[6] Lande D., Shnurko-Tabakova E. OSINT as a part of cyber defense system // Theoretical and Applied Cybersecurity. — 2019. — no. 1. — P. 103–108.

[7] J. Kleinberg. Temporal dynamics of on-line information streams. — Spriger, Berlin, Heidelberg, 2006. — ISBN: 978-3-540-28608-0.

[8] Fundamentals of modeling and evaluation of electronic information flows (in Russian) / D. V. Lande, V. N. Furashev, S. M. Braichevskiy, A. N. Grigoriev. — Kyiv, Inzhiniring, 2006.

[9] Singh R., Reddy V. Personalized recommendation of Twitter lists using content and network information // Proceedings of the ACM on Human-Computer Interaction. — 2014. — 5. — Vol. 8, no. 1. — P. 416–425.

[10] Dodonov O. G., Lande D. V., Gorbulin V. P. Information Operations and security of society: threats, counteraction, modeling (in Ukrainian). — K.:Intertekhnologiia, 2009.

[11] Astafieva N. Wavelet analysis: bases of the theory and examples of application // Achievements of physical sciences. — 1996. — no. 11. — P. 1145–1170.

[12] A.Davydov. Wavelet analysis of social processes // Sociological researches. — 2003. — no. 11. — P. 97–103.