CYBERSECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

DOI 10.20535/2411-1031.2021.9.2.249921
УДК 004[942+056.5]

OLEKSANDR PUCHKOV,
DMYTRO LANDE,
IHOR SUBACH,
MYKHAILO BOLIUKH,
DMYTRO NAHORNYI

OSINT INVESTIGATION TO DETECT AND PREVENT CYBER ATTACKS AND CYBER SECURITY INCIDENTS

A methodology for investigating and predicting cyber incidents based on the use of open sources of information and freely available open source software is offered and substantiated. The suggested methodology refers to such types of methodologies as Open Source Intelligence (OSINT). In addition, it is based on technologies of monitoring the modern Internet space, the concept of processing large amounts of data (Big Data), complex networks (Complex Networks), and extracting knowledge from text arrays (Text Mining). The components of the keyword detection technology (NLTK, Natural Language Toolkit), concepts (SpaCy, NLP), graph visualization and analysis systems are considered in detail. The main idea of analyzing large amounts of data on cybersecurity from the Internet space is to use methods and tools for collecting data using global search engines, aggregating information flows and mining the data obtained. The technique is based on the implementation of such functions as the collection of relevant information from certain information resources using the capabilities of global search engines; automatic scanning and primary processing of information from websites; formation of full-text arrays of information; analysis of text messages, determination of sentiment, formation of analytical reports; integration with a geographic information system; analysis and visualization of information reports; research of dynamics of thematic information flows; forecasting the development of events based on the analysis of the dynamics of publications in the Internet space. In the analytical mode, a number of tools are implemented for graphical presentation of data dynamics, displayed as a time series of the number of messages per day matching to a specific cyber incident, viewing plots from messages on the topic of cyber incidents, clusters grouped by the cluster analysis algorithm. Within the framework of the methodology, it is provided for the formation and inclusion of networks in operational reports from concepts matching to people, organizations, information sources, allowing to explore the relationship between them.

Keywords: cyber security, cyber security incident, open source intelligence, big data.

Problem Statement. The relevance of solving the scientific problem, which is considered in the article, is in the necessity to develop a solution for automating Open Source Intelligence (OSINT), which would include collecting, processing and analyzing information, extracting concepts (notions), determining the relationship of these concepts, displaying events on a geographic map, analysis and forecasting future cyber incidents, generation of reports based on this information for decision-makers, cybersecurity subjects.

The practical lack of automated OSINT tools at the operational and technical level of cybersecurity combined with the lack of common approaches to open source intelligence leads to increased response time to cyber incidents and reduced efficiency of relevant analytical units [1] - [3].

According to these circumstances, the methodology of investigation and forecasting of cyber incidents based on open source information and freely available open source software that provides investigation of cyber incidents that have already occurred, collection of analytical data on them,

accumulation of relevant analytical information for future application of machine learning methods and technologies, timely detection of cyberattacks currently underway, research and prediction of future cyberattacks, is an urgent scientific task.

The purpose of the article is to provide the user with a working science-based methodology and available software solution for OSINT, which allows you to: analyze cyber attacks and cyber incidents that have already happened; analyze current cyberattacks; collect analytical information for the research and predict probable cyberattacks.

The main material research. Suggested approach [4] - [10]. To solve the formulated scientific problem, a new method is offered, which involves the following actions:

1) Determining the time interval [T1, T2] when the cyber incident was committed. This information can be found in official sources, reports of cyberattacks, online media reports, etc.
2) Obtain, as far as possible, the largest number of links to messages from the Internet web resources related to the specified cyber incident in the time interval [T1 – C, T2 + C], where C is a constant, for example, which matches to 30 days.
3) Obtaining full texts of all messages that matched to the links and their pre-processing.
4) Aggregation of received messages by the time of their appearance on the Internet, construction of a time series of publications dynamics on the topic of a particular cyber incident.
5) Research of the received time series, smoothing, carrying out the wavelet analysis, receiving the scalogram, detection of anomalies, periodicity, etc., comparison with known patterns of information operations and cyber incidents.
6) Obtaining from the texts of concepts – named entities, geographical names (toponyms), names and surnames of people and names of organizations. Display on the map the toponyms that matched to the selected cyber incident.
7) Building a network of these entities, identifying the most related groups.
8) Building digests from messages.

To research cyber incidents that occur at this time, it is necessary to perform almost all of these steps (step 2 in case when T2 is unknown), then perform time series prediction, for example, by Sornette method [9], [10] to predict future cyber incident behavior.

Such software solution consists of a client web application and a server part for data processing, which contains the REST API and a data processing module using open Python libraries. The Elasticsearch system is used to accumulate analytical information for further use and machine learning [4].

A practical example of cyber incident investigation. Let us demonstrate the application of the suggested method using the example of the well-known cyber attack of 2021, namely the cyberattack on the Colonial Pipeline – the use of malware software to disable the American Colonial Pipeline system. On May 7, 2021, this cyberattack shut down all pipelines in the system for five days. As a result, US President Joe Biden declared a state of emergency. According to press reports, this is "the most successful cyber attack on oil infrastructure in the history of the country". Open sources reported that the cyberattack was carried out by a group of DarkSide hackers. It is believed that the day before the cyber attack, the same group stole 100 gigabytes of data from the company's servers. The operation of the pipeline was fully computerized. Colonial Pipeline's technical management system has been integrated with the administrative system, which opens up potential opportunities for the Internet penetration, most of all with the help of using e-mail. This vulnerability is usually exploited by cyber attackers. A few days after the shutdown of the pipeline in the coastal states of the Southeastern United States, a shortage of gasoline and diesel fuel began. On May 12, 71% of gas stations were closed due to fuel shortages. On May 14, 88% of gas stations in Washington were without petrol. Retail gasoline prices in the United States reached a ten-year high. The fuel shortage ended a few days after the pipeline resumed operation. According to the FBI, the DarkSide criminal group was involved in the attack.

The first step: the date of the cyber incident. According to information from open sources on the Internet, data about this cyber attack is found in the period of time [T1, T2]. In particular, it is

determined that the cyberattack was carried out during May 6-12, 2021. We select a range of dates for scanning. Usually, a period starting one month before the day of the attack start is sufficient; and ends one month after the day the attack ends. Having determined the constant C = 30 days, we set the date interval for scanning: April 4, 2021 – June 12, 2021.

The second step: creating an array of relevant information. In accordance with paragraph 2 of the methodology, electronic documents are collected that correspond to a given topic for a certain period. These documents were sourced from Google, GoogleNews and Bing searches for the keywords "Colonial Pipeline Cyberattack" for the above time interval. A total of 1817 references to documents, which were collected by the Selenium WebDriver system using a program module developed by the Python language, were found.

The third step: preparing the collected documents for analysis. Collected messages are formatted according to the state, which is suitable for further analysis. The full texts of the messages matching to the links were pre-processed, cleaned of HTML-tags, fragments of JavaScript-code, advertising parts, etc. In this case, there is only the useful content of the message, so pre-processing of message texts and their normalization was conducted.

The fourth step: dynamics of publications**.** The notifications received in the previous stage were published at different times. If you aggregate messages by the time of their appearance on the Internet (by date), a time series of dynamics of publications on the topic of a particular cyber incident will be built. Each item in this series matchs to the number of messages on a particular topic that appeared on the Internet on a given date. This series has a feature – a clear weekly harmonica associated with the natural dynamics of publications. Smoothing this series helps to identify significant trends in the dynamics of the series, while hiding the noise and various features that are manifested on a small scale. For smoothing, the moving average method was chosen for the window [5], [6], with a window size of 7 (the number of days in a week). After that, graphs of the dynamics of publications are displayed. For this, a software application developed in the Python language is used (fig. 1).

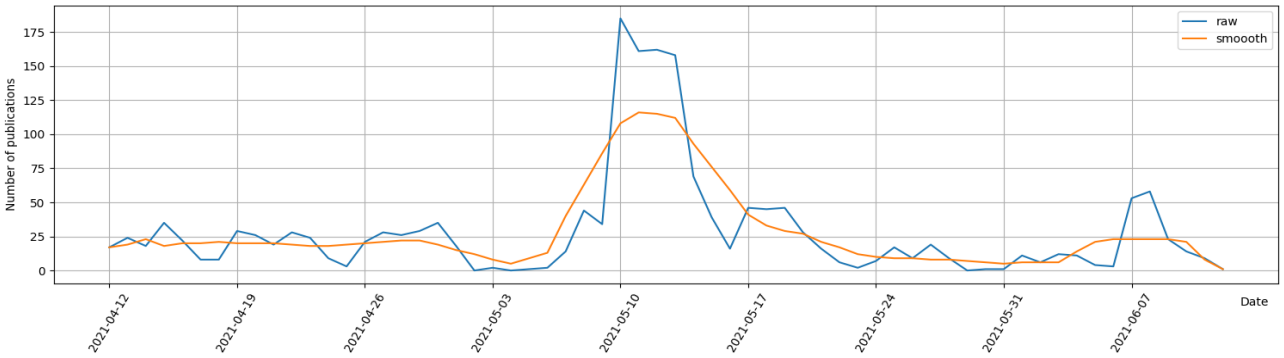


Figure 1 – Output and smoothed rows

The fifth step: wavelet analysis. To identify the similarity of fragments of the studied time series at different scales, wavelet analysis is used [7], [8].

The main idea of wavelet analysis is that the time series are divided into separate observation windows, on each of which a value is calculated that shows the degree of closeness of the patterns of the studied data to the different shifts of some special function (wavelet) at different scales.

In the course of the wavelet analysis, a certain wavelet function ψ (t) is selected, with which the original function x (t) is compared by the formula:

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

where $l,s\in\Re,s\neq 0;\psi^{*}-$ the function is complexly related to ψ, and the quantities $\{W(s,l)\}\_(l,s\in\Re)$ are called wavelet transform coefficients (wavelet coefficients).

In this case, it was decided to use the MexH wavelet (Mexican hat), as it is close in form to the diagram of any information operation (fig. 2).

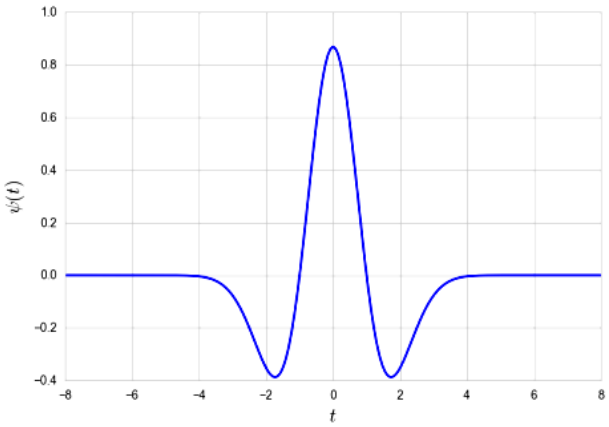


Figure 2 – MexH wavelet (Mexican hat)

The obtained wavelet coefficients can be represented graphically if the wavelet shifts (time axis) are plotted along one axis, and scales (scale axis) along the other; and the points of the resulting scheme are colored depending on the value of the corresponding coefficients.

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

Wavelet analysis allows you to check the time series for compliance with the most suitable templates for describing cyberattacks and information operations. In fig. 3, a wavelet scale chart of a time series describing the dynamics of publications on a given topic is shown. It can be seen that the time series quite clearly correspond to the MexH template on a large scale. The time series scaling shows two distinct anomalies: a bright spot indicating the active phase of the cyber incident, and a less bright spot after the attack, the "investigation" phase. The first date anomaly falls on the dates of the attack, and the second falls on the period from June 6 to 11, 2021. Also, the scale chart clearly shows the weekly frequency of publications.

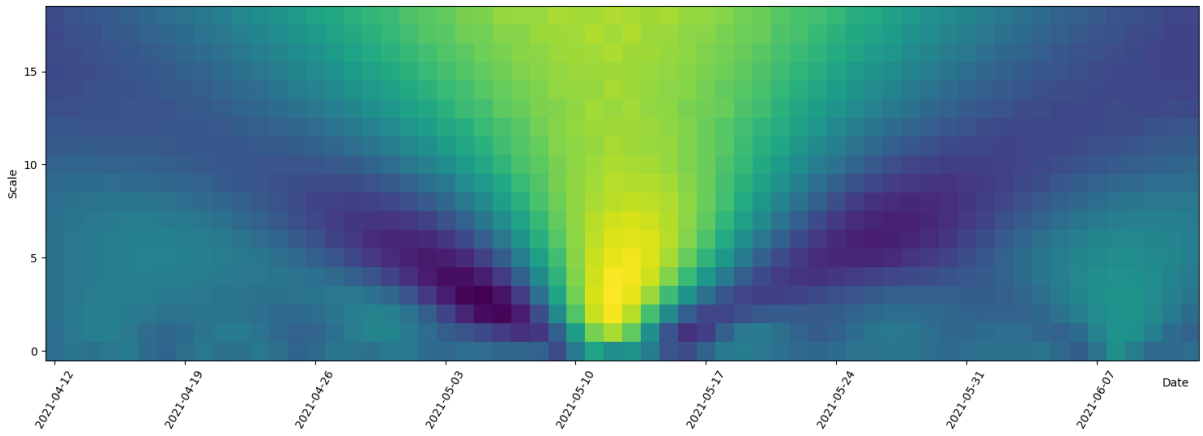


Figure 3 – Scalelogram of the time series based on the MexH wavelet

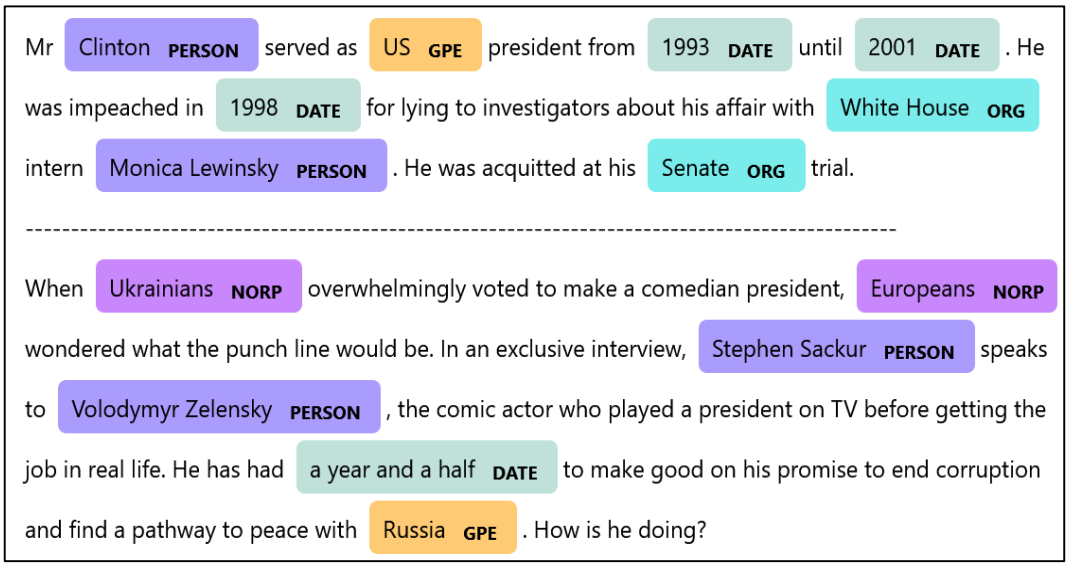
The sixth step: forecasting the time series. The possibility of forecasting ("Forecast") is provided by the method offered by D. Sornett [9], [10], which is based on the analysis of the patterns of market prices movement in commodity and stock markets before the crash. The corresponding power-law model, taking into account linear log-periodic oscillations, has the following form:

$$F(t) = A + B(t_c - t)^m \left[1 + C\cos\left(\omega \log\left(\frac{t_c - t}{T}\right) + \varphi\right)\right],$$

where $F(t)$ is a power-law model taking into account log-periodic fluctuations;

t_c – critical time;

A, B, ω, φ – coefficients of the model determined by fitting. Based on the use of the Sornette model and monitoring data, the predicted values of the corresponding publications can be obtained.



a)

	Persons			Organisations	
№	Entity	Count	№	Entity	Count
1.	Joe Biden	759	1.	Colonial Pipeline	2899
2.	Joseph Blount	181	2.	FBI	499
3.	Jennifer Granholm	130	3.	White House	192
4	Roy Cooper	84	4.	Congress	174
5.	Charlotte Hornets	72	5.	Reuters	168
6.	Vladimir Putin	73	6.	Microsoft	140
7.	Darkside	70	7.	CISA	139
8.	Patrick De Haan	58	8.	GasBuddy	131
9.	Lisa Monaco	53	9.	AAA	138
10.	Anne Neuberger	51	10.	SolarWinds	123

b)

Figure 4 – An example of detecting concepts in the information message:
a) automatic message marking; b) concept discovery

The seventh step: selection of entities. To identify concepts (notions), “template” techniques are now widely used, which apply template libraries that are most often used to designate concepts in the texts of information messages. At the same time, more and more often machine learning and pattern recognition methods are used when training such systems. One of the approaches to creating systems is to use open source software libraries, in particular, the Python library spaCy.

Below is a list of concepts that cover the spaCy system. PERSON: People, including fictional.

NORP: Nationalities, religious or political groups. FAC: Buildings, airports, highways, bridges, etc. ORG: Companies, agencies, institutions, etc. GPE: Countries, cities, states. LOC: Non-GPE locations, mountain ranges, bodies of water .PRODUCT: Objects, vehicles, food, etc. (Not services.) EVENT: Named hurricanes, battles, wars, sports events, etc. WORK_OF_ART: Titles of books, songs, etc. LAW: Named documents made into laws. LANGUAGE: Any named language.

DATE: Absolute or relative dates or periods. TIME: Times smaller than a day. PERCENT: Percentage, including ”%“. MONEY: Monetary values, including unit. QUANTITY: Measurements, as of weight or distance. ORDINAL: “first”, “second”, etc. CARDINAL: Numerals that do not fall under another type. In fig. 4 an example of detecting concepts in an information message is shown.

Entities of various types are removed from formatted messages. For the current analysis, the entities are used: personality, organization, geographic tag. The resulting sets are ranked according to the number of occurrences in the documents for the prepared sample. Tables 1 and 2 provide a list of the 10 most frequently used individuals and organizations, respectively.

Table 1 – Personalities

№	Personality	Number of occurrences
1.	Joe Biden	759
2.	Joseph Blount	181
3.	Jennifer Granholm	130
4.	Roy Cooper	84
5.	Charlotte Hornets	72
6.	Vladimir Putin	73
7.	Darkside	70
8.	Patrick De Haan	58
9.	Lisa Monaco	53
10.	Anne Neuberger	51

Table 2 – Organizations

№	Organization	Number of occurrences
1.	Colonial Pipeline	2899
2.	FBI	499
3.	White House	192
4.	Congress	174
5.	Reuters	168
6.	Microsoft	140
7.	CISA	139
8.	GasBuddy	131
9.	AAA	138
10.	SolarWinds	123

Table 3 lists the 20 geotags most frequently mentioned in documents.

Table 3 – Geotags

№	Geotag	Number of occurrences	№	Geotag	Number of occurrences
1.	US	5075	11.	New York	439
2.	Russia	811	12.	Washington	418
3.	North Carolina	726	13.	Canada	367
4.	Georgia	670	14.	New Jersey	352
5.	Israel	643	15.	Atlanta	309
6.	Texas	592	16.	India	308
7.	Virginia	513	17.	South Carolina	290
8.	NC	489	18.	California	286
9.	Florida	483	19.	Tennessee	235
10.	China	460	20.	New York	439

The list of entities includes geographic information associated with a related topic. Geo-tags (names of countries, cities) found in the relevant topics of messages are displayed on a geographic map. To extract and display geotags, a program module developed by the Python language is used that publishes geographical names, as well as geographical coordinates (latitude, length). A fragment of the web interface with the display of geotags on a geographic map for visualization is shown in fig. 5.

Next, relationships are established between the entities identified earlier. Entities are considered linked if they occur simultaneously in the same messages. The weight of a relationship is determined by the number of messages containing both entities at the same time. The size of a node corresponding to an entity is proportional to its degree. To build networks of entities, a special software module was used, the result of which is a data set in CSV format, corresponding to an adjacency matrix. It is displayed using the Gephi graph visualization and analysis system.

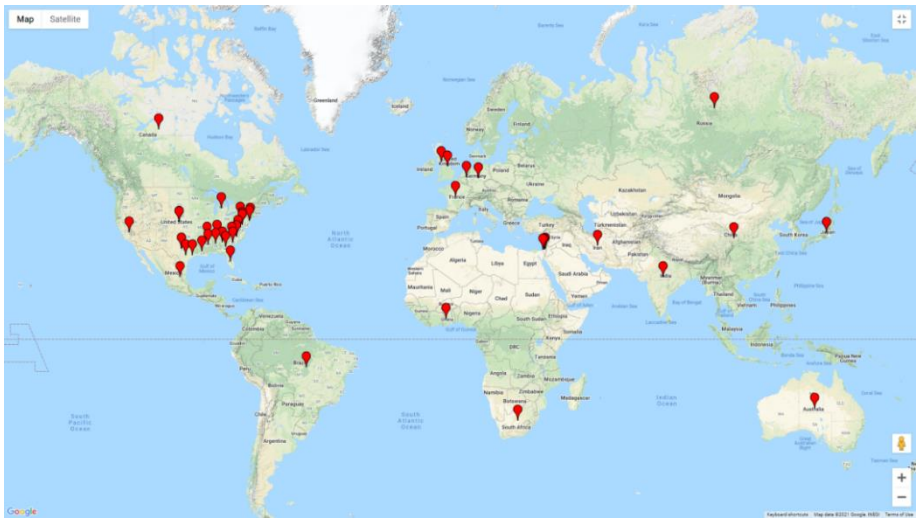
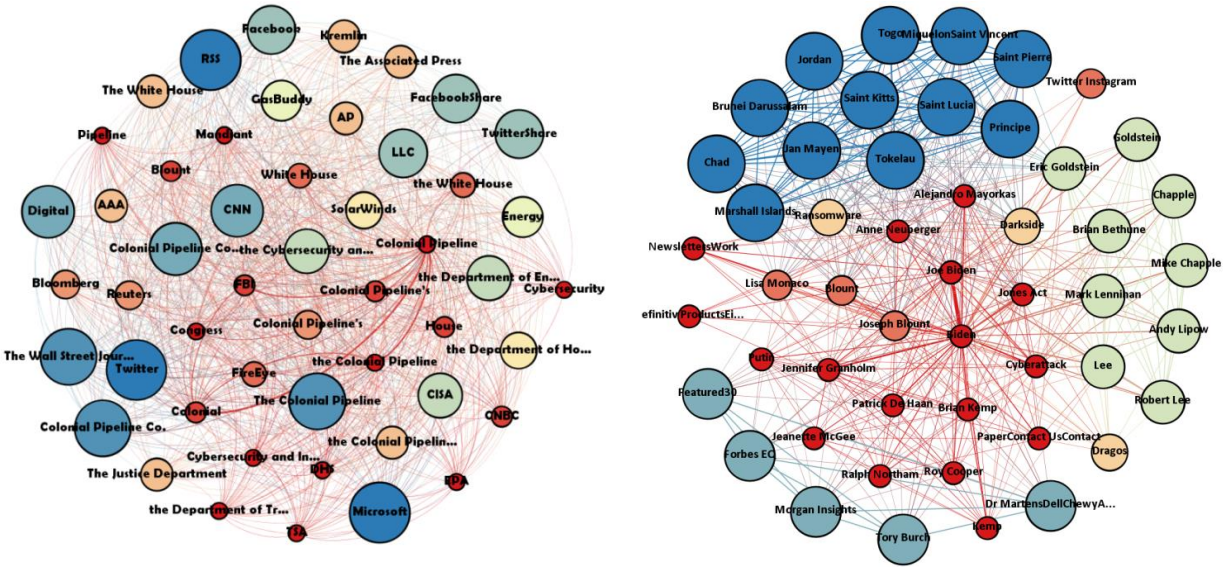


Figure 5 – Displaying geotags on the map

The generated CSV file opens in the Gephi application. Groups (clusters) are identified by the criterion of modularity [11].



a) b)

Figure 6 – Graphs of relationships: (a) – “organization-organization”, (b) – “person-person”

In fig. 6 graphs of relationships between entities are shown.

№	Content	URL-link
1	Colonial Pipeline ransomware updates. Warnings on Avaddon, Babuk ransomware. Lemon Duck cryptojacker. Bogus Chrome app.	https://thecyberwire.com/newsletters/daily-briefing/10/90
2	Privately owned Colonial Pipeline opened portions of the line manually in Georgia, Maryland, New Jersey and the Carolinas. It also accepted two million barrels.	https://www.cbc.ca/news/business/fuel-shortages-southeastern-us-pipeline-1.6023362
3	Fuel prices spiked and states of emergency were put in place across various states in the Southeastern U.S. after a cyberattack on Colonial Pipeline.	https://www.washingtonpost.com/business/2021/05/12/gas-shortage-colonial-pipeline-live-updates/
4	The Colonial Pipeline, a major U.S. fuel pipeline along the East Coast, was hit by a cyberattack on Friday. The company halted operations after revealing.	https://www.ktvu.com/news/colonial-pipeline-attack-amid-service-outage-nc-declares-state-of-emergency-to-help-ensure-fuel-supply

Figure 7 – Fragment of the digest on the topic ”cyberattacks on the Colonial Pipeline”

Step 8: forming the digest. Based on the collected data, a digest is formed – a list of relevant documents reflecting various the most important aspects of a particular cyber incident. Digests include documents from a selected array for different dates, containing the largest number of valid entities identified in the previous stages. An example of a digest that is generated automatically using a separate program module in Python is shown in fig. 7.

Conclusions. Thus, the scientific methodology and information technology for the implementation of OSINT for the detection and investigation of cyber attacks and cyber incidents are suggested. Its main advantages are a high level of document orientation by topic, low implementation, deployment, and support costs.

The data obtained during processing with the above mentioned software application is a source of information for investigating and predicting cyberattacks by identifying patterns of their implementation.

The example given in this paper analyzes the news publishing dynamics on the topic of ”cyber attacks on the Colonial Pipeline”. The conducted wavelet analysis of the time series showed its correspondence to the templates used to describe cyberattacks and information operations. It confirmed the existence of an attack in the period April 6 – June 12, 2021, and the peak, which fell on June 6 – 11, 2021, most likely corresponds to the period of analysis of the cyberattack consequences. This period is characterized by an increase in the publications dynamics in connection with the publication of materials on the investigation of this cyber incident.

REFERENCES

[1] D. Lande, and E. Shnurko-Tabakova, “OSINT as a part of cyber defense system”, *Theoretical and Applied Cybersecurity*, no. 1, pp. 103-108, 2019, doi: https://doi.org/10.20535/tacs.2664-29132019.1.169091.

[2] B. Akhgar, P. S. Bayerl, and F. Sampson, *Open Source Intelligence Investigation. From Strategy to Implementation*. Cham: Springer International Publishing AG, 2016.

[3] N. Memon, and R. Reda Alhajj, *Counterterrorism and Open Source Intelligence*. Wien, Austria: Springer-Verlag, 2011.

[4] D. Lande, I. Subach, and A. Puchkov, “System of Analysis of Big Data from Social Media”, *Information & Security: An International Journal*, vol. 47, no. 1, pp. 44-61, 2020, doi: https://doi.org/10.11610/isij.4703.

[5] D. V. Lande, I. Yu. Subach, and Yu. Ye. Boyarinova, *Fundamentals of the theory and practice of data mining in the field of cyber security*. Kyiv: Institute of Special Communications and Information Protection of National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, 2018.

[6] D. Lande, “Information Streams Analysis in the Global Computer Networks”, *Visnyk NAS of Ukraine*, no. 3, pp. 46-54, 2017, doi: https://doi.org/10.15407/visn2017.03.045.

[7] N. Astafieva, “Wavelet analysis: bases of the theory and examples of application”, *Achievements of physical sciences*, iss. 11, pp. 1145-1170, 1996.

[8] A. Dodonov, D. Lande, V. Tsyganok, O. Andriichuk, S. Kadenko, and A. Graivoronskaya, *Information Operations Recognition. From Nonlinear Analysis to Decision-Making.* Kiev: Lambert Academic Publishing, 2019.

[9] D. Sornette, *Why Stock Markets Crash: Critical Events in Complex Financial Systems*. Princeton: Princeton University Press, 2004, doi: https://doi.org/10.23943/princeton/9780691175959.001.0001.

[10] D. Sornette, *How to predict the collapse of financial markets. Critical events in complex financial systems.* Princeton: Litres, 2017.

[11] D. Lande, and I. Subach, *Visualization and analysis of network structures*. Kyiv: National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Politekhnika, 2021.

The article was received 21.09.2021.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] D. Lande, and E. Shnurko-Tabakova, "OSINT as a part of cyber defense system", *Theoretical and Applied Cybersecurity*, no. 1, pp. 103-108, 2019, doi: https://doi.org/10.20535/tacs.2664-29132019.1.169091.

[2] B. Akhgar, P. S. Bayerl, and F. Sampson, *Open Source Intelligence Investigation. From Strategy to Implementation*. Cham: Springer International Publishing AG, 2016.

[3] N. Memon, and R. Reda Alhajj, *Counterterrorism and Open Source Intelligence*. Wien, Austria: Springer-Verlag, 2011.

[4] D. Lande, I. Subach, and A. Puchkov, "System of Analysis of Big Data from Social Media", *Information & Security: An International Journal*, vol. 47, no. 1, pp. 44-61, 2020, doi: https://doi.org/10.11610/isij.4703.

[5] Д. В. Ланде, І. Ю. Субач, та Ю. Є. Бояринова, *Основи теорії і практики інтелектуального аналізу даних в сфері кібербезпеки*. Київ: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2018.

[6] D. Lande, "Information Streams Analysis in the Global Computer Networks", *Visnyk NAS of Ukraine*, no. 3, pp. 46-54, 2017, doi: https://doi.org/10.15407/visn2017.03.045.

[7] N. Astafieva, "Wavelet analysis: bases of the theory and examples of application", *Achievements of physical sciences*, iss. 11, pp. 1145-1170, 1996.

[8] A. Dodonov, D. Lande, V. Tsyganok, O. Andriichuk, S. Kadenko, and A. Graivoronskaya, *Information Operations Recognition. From Nonlinear Analysis to Decision-Making.* Київ: Lambert Academic Publishing, 2019.

[9] D. Sornette, *Why Stock Markets Crash: Critical Events in Complex Financial Systems*. Princeton: Princeton University Press, 2004, doi: https://doi.org/10.23943/princeton/ 9780691175959. 001.0001.

[10] D. Sornette, *How to predict the collapse of financial markets. Critical events in complex financial systems.* Princeton: Litres, 2017.

[11] Д. Ланде, та І. Субач, *Візуалізація та аналіз мережевих структур*. Київ: ІСЗЗІ КПІ ім. Ігоря Сікорського, Політехніка, 2021.

ОЛЕКСАНДР ПУЧКОВ,
ДМИТРО ЛАНДЕ,
ІГОР СУБАЧ,
МИХАЙЛО БОЛЮХ,
ДМИТРО НАГОНИЙ

OSINT-РОЗСЛІДУВАННЯ ДЛЯ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ КІБЕРАТАКАМ ТА ІНЦИДЕНТАМ КІБЕРБЕЗПЕКИ

Запропоновано та обґрунтовано методика розслідування і прогнозування кіберінцидентів на базі застосування відкритих джерел інформації і вільно доступного програмного забезпечення з відкритим кодом. Запропонована методика відноситься до методологій типу Open Source Intelligence (OSINT). Крім того, вона базується на технологіях моніторингу сучасного інтернет-простору, концепції обробки великих обсягів даних (Big Data), складних мереж (Complex Networks), добування знань із текстових масивів (Text Mining). Детально розглянуті компоненти технології виявлення ключових слів (NLTK, Natural Language Toolkit), понять (SpaCy, NLP), системи візуалізації і аналізу графів. Основна ідея аналізу великих обсягів даних з питань кібербезпеки з Інтернет-простору полягає у застосуванні методів і засобів збирання даних із застосуванням глобальних пошукових систем, агрегування інформаційних потоків та інтелектуального аналізу добутих даних. Методика базується на реалізації таких функцій, як збір релевантної інформації з визначених інформаційних ресурсів із використанням можливостей глобальних пошукових систем;

автоматичне сканування і первинна обробки інформації з веб сайтів; формування повнотекстових масивів інформації; аналіз текстових повідомлень, визначення тональності, формування аналітичних звітів; інтеграцію з географічною інформаційною системою; аналіз та візуалізацію інформаційних звітів; дослідження динаміки тематичних інформаційних потоків; прогнозування розвитку подій на основі аналізу динаміки публікацій в Інтернет-просторі. В аналітичному режимі реалізовано низку інструментів для графічного представлення динаміки даних, які відображуються у вигляді часового ряду кількості відповідних конкретному кіберінциденту повідомлень за добу, перегляду сюжетів із повідомлень за темою кіберінцидентів, кластерів, що згруповані за алгоритмом кластерного аналізу. У рамках методики передбачено формування і включення до оперативних зведень мереж із концептів, що відповідають персонам, організаціям, інформаційним джерелам, які дозволяють досліджувати взаємозв'язки між ними.

Ключові слова: кібербезпека, кіберінцидент, розвідка з відкритих джерел, великі дані.

Пучков Олександр Олександрович, кандидат філософських наук, професор, начальник, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-8585-1044, iszzi@iszzi.kpi.ua.

Ланде Дмитро Володимирович, доктор технічних наук, професор, завідувач кафедри інформаційної безпеки Навчально-наукового Фізико-технічного інституту Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0003-3945-1178, dwlande@gmail.com.

Субач Ігор Юрійович, доктор технічних наук, доцент, завідувач кафедри кібербезпеки і застосування інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-9344-713X, igor_subach@ukr.net.

Болюх Михайло Олександрович, магістрант, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0001-8984-7686, mishytka442000@gmail.com.

Нагорний Дмитро Олександрович, магістрант, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-3699-7880, dmytro.nahornyi@ukr.net.

Puchkov Oleksandr, candidate of philosophy science, professor, head of Institute of special communications and information protection of National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Lande Dmytro, doctor of technical science, professor, head of the information security academic department, Institute of physics and technology of National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Subach Ihor, doctor of technical science, associate professor, head of the cybersecurity and application of information systems and technologies academic department, Institute of special communications and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Boliukh Mykhailo, master's student, Institute of special communications and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Nahornyi Dmytro, master's student, Institute of special communications and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.