System for Monitoring the Connection of USB Devices for Cybersecurity Auditing

Vadym Kalchenko [1] [0000-0001-6492-3806], Nataliia Barchenko [1] [0000-0002-5439-8750], Andrii Tolbatov [2] [0000-0002-9785-9975], Victor Obodiak [1] [0000-0002-8539-1252], Volodymyr Tolbatov [1] [0000-0002-6564-9658] and Vadym Tatarinov [1] [0000-0003-0677-2776]
Sergiy Gnatyuk[3,4,5] [0000-0003-4992-0564]

[1] Sumy State University, Sumy, Ukraine
[2] Sumy National Agrarian University, Sumy, Ukraine
[3] National Aviation University, Kyiv, Ukraine
[4] State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, Kyiv, Ukraine
[5] Yessenov University, Aktau, Kazakhstan

s.gnatyuk@nau.edu.ua

Abstract. The paper considers the urgent task of ensuring information security by monitoring the connections of USB devices. An analysis of the available solutions was carried out, and technologies were identified that will allow the system to be implemented. The topology of the physical components of the system is developed and described. The subject area model is described by an ER diagram that contains key entities and links them. The description of model attributes is given. The system is implemented in the form of two Windows services, utilities for configuring launch options for services and a web application. The verification plan is given, according to which the system was proved to be operational. The developed system can be recommended for solving the urgent cybersecurity task of monitoring device connectivity.

Keywords: cybersecurity measures, information protection, connection to the USB port.

1 Introduction

At the present stage, information is becoming one of the most valuable and sought-after resources, for the preservation and protection of which more and more time and money is allocated. In this regard, a cybersecurity measure to protect information is one of the important processes of any organization. The process of information security management is inextricably linked with the monitoring of events in the system. Availability, small size and increased capacity of USB drives casts great doubt on the information security of companies. Ignoring this threat can lead to significant material losses. By connecting to a USB port, an attacker can snatch im-

 CybHyg-2019: International Workshop on Cyber Hygiene, Kyiv, Ukraine, November 30, 2019.

portant information or install malware. More and more companies are investing in firewalls, using more reliable and modern encryption algorithms, and other means and technologies to protect data from Internet theft. However, the most common attackers are employees of the company, who steal information about investments, project documents, commercial offers, personal information and contact details of customers and much more.

Disconnecting USB ports is a radical security measure that will lead to significant inconvenience and inability to connect peripherals to your computer. Determining the list of allowed devices using a serial number is a good measure to prevent information leakage, but not enough. The serial number of the flash drive can be changed to any, which will allow the infringer to access important data without any obstacles.

An important security measure is to monitor the connection of USB devices to corporate computers. Centralized connection tracking is an effective way to investigate leaks via USB devices, allowing security management or the security administrator to respond in a timely manner and identify the device, date, time, and computer where the incident occurred. Analysis of this data and detection of the fact of connection of the device will help to successfully identify the attacker and take the necessary measures.

The aim of the work is to increase the efficiency of information protection systems by developing a subsystem for monitoring the connection of USB-devices.

2 Related works analysis and problem statement

One of the important tasks of modern information and / or cybersecurity systems is to ensure promptness (timeliness) in identifying threats and risks for information objects and processes to be protected. In order to increase efficiency in information and / or cybersecurity management systems, components are used that record changes in the functional state of an object or process automatically. The basis of such components are high-quality agents (hardware or software) to collect data on the current state of individual components of the object or process and effective agents that can analyze the collected data and make decisions about the functional state of the object or process as a whole. Examples of the first type of agents are in [1]. Implementation of agents of the second type requires the involvement of machine learning technologies [2] and pattern recognition similar to those used in intelligent decision support systems for technological, economic, environmental, and social objects or processes.

Large companies and corporations use Security Information and Event Management (SIEM) technology for cybersecurity [3-11] systems based on this technology, enable the centralized collection and analysis of security relevant information, generated by a variety of different systems, to detect advanced threats and to improve reaction time in case of an incident.

According to [4, 5, 7, 11]:

- Security information management (SIM) — log management and compliance reporting.
- Security event management (SEM) — real-time monitoring and incident management for security-related events from networks, security devices, systems, and applications [12-15].

However, small companies do not have the opportunity to invest heavily in ensuring information security on this technology and conducting training of specialists for the quality performance of their functions in the application of the above products. During the analysis of existing solutions, software products were identified that can fully or partially perform the task monitoring of USB device connections: USB Canary, USBDeview, CleverControl, Solarwinds Security Event Manager, and AlienVault.

Determine the main characteristics of the monitoring system USB connections, which meet the needs of a small company, and determine the compliance of existing solutions to these requirements (see Table 1).

Thus, a review of existing solutions has shown that both paid and free products can be used to monitor USB device connections. The disadvantage of free solutions is the lack of functionality that does not meet all the needs for a full-fledged solution. Most free solutions do not have a centralized analysis of events when connecting USB devices to corporate computers. Paid versions contain redundant features that you have to pay for.

Therefore, it is necessary to develop a system that will:

- track connection events on corporate computers;
- provide centralized collection and storage of events for further analysis;
- have an intuitive web interface for easy viewing and analysis of events;
- provide the ability to find the right events;
- access to view events must be carried out after the authorization procedure;
- the ability to manage users of the web application and delete irrelevant information. Access to these functions should be provided only to users with administrator rights.
- ability to recover the password;
- ability to deploy the program on the computer to be monitored.

Table 1 - Comparison of available solutions

Criterion	Solution				
	USB Canary	USBDeview	CleverControl	Solarwinds Security Event Manager	Alien Vault
You can deploy on your own computers	+	+	-	+	-
Centralized viewing of events	-	-	+	+	+
Ability to view the history of events	-	-	+	+	+
Viewing of USB device data and node data	-	+/-	+	+	+

Criterion	Solution				
	USB Canary	USBDeview	CleverCon-trol	Solarwinds Security Event Manager	Alien Vault
(MAC, IP, etc.)					
It has insuffi-cient function-ality	+	+	-	-	-
Contains re-dundant fea-tures	-	-	+	+	+
Windows sup-port	-	+	+	+	+
Clear interface	-	+	+	+	+
Price	Free of charge	Free of charge	From 180$ / year	From 4.805$ for 30 nods / year	1075$/ Month

Tasks to be solved to achieve these requirements [16-18]:

- analyze the subject area;
- choose the means to develop the system;
- configure the environment for software development;
- develop a customer service to monitor USB devices;
- develop a server service for centralized collection of events and their recording in the database;
- design the structure of the database;
- develop a web application for convenient viewing of events and analysis of events;
- test the system.

3 Modeling of the subject area

For high-level design of databases ER-chart was developed. This model allows you to describe the subject area, highlight key entities, and identify the relationships that can be established between those entities.

Figure 1 shows a database diagram that meets the requirements of the development system. In order to avoid potential inconsistencies and redundancy of the data, the model was reduced to the third normal form during the design.

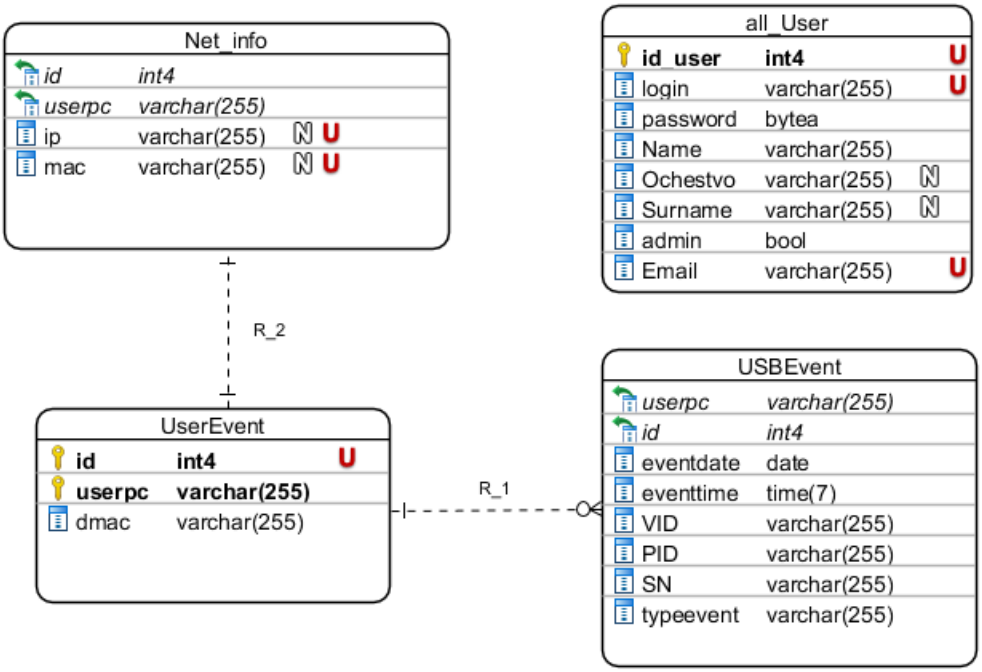

Fig. 1. - ER diagram of the system database

Description of the attribute values is given in Table 2.

Table 2 - Description of attributes

Table	Field	Keys	Content
All_User	Id_user	PK	Stores a number that uniquely identifies the instance of the entity
	login		Saves the login of the web application user
	password		Saves the password for the web application user
	Name		Web application username
	Surname		Last name of the web application user
	Otchestvo		Web application user patronymic

Table	Field	Keys	Content
	admin		Shows the presence or absence of administrator rights
	email		Web application user email address
USBEvent	Id	FK	Saves a number that uniquely identifies the entity instance, allows you to link tables
	userpc	FK	Ethernet card MAC address
	eventdate		Date of the event
	eventtime		Time of the event
	vid		USB drive manufacturer number
	pid		USB drive model number
	SN		The serial number
	typeevent		Event type (connect or disconnect)
Net_info	Id	FK	Saves a number that uniquely identifies an entity instance, allows you to link tables
	userpc	FK	Ethernet card MAC address
	ip		Current IP address of the corporate computer
	mac		MAC address of the corporate computer

To display the topology of physical components of the system and the location of software components of the system, a deployment diagram was developed (Fig. 2). Using this diagram, you can display the location of complex information systems that require different computing platforms and database access technologies. This makes it possible to streamline the placement of components in the corporate network, which determines the overall performance of the system. The need to integrate systems with the Internet requires addressing related security issues and the availability of information for corporate customers. The use of "client-server" technology requires the placement of large databases in different segments of the corporate network, their archiving, backup, and hashing, which in turn will ensure system performance. These

aspects also require visual representation to specify the software and technical features of the implementation of distributed architectures.

Hereof it is possible to allocate the basic purposes of development of the deployment diagram:

- distribute the components of the system on physical nodes;
- show physical connections between nodes during execution;
- facilitate the system configuration process.

The main component of the deployment diagram are nodes and their relationships. Representation of nodes occurs by means of rectangular parallelepipeds with the artifacts which are located in them. In turn nodes can contain the subnodes, presented by rectangular parallelepipeds. A node on the deployment duagram can rearrange a computer, a database server, network components, and other.

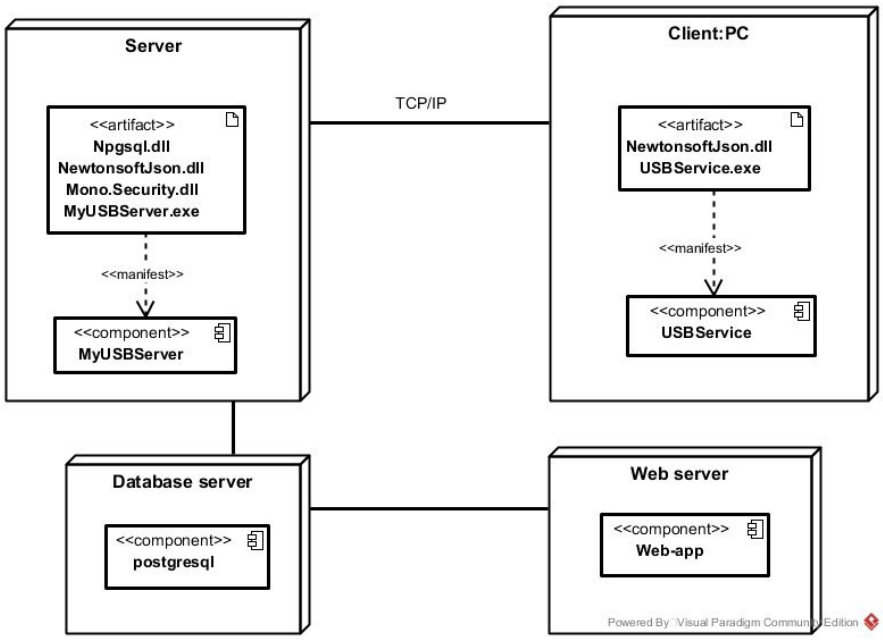

Fig. 2. – Deployment diagram of the monitoring system for USB device connection

The diagram shows four physical nodes:

- server - a node on which the server service is located;
- client - a node over which monitoring is carried out, and on which the client service is located. Any corporate computer can be this node;
- web server - a node on which the web application is installed, the main purpose of which is to analyze events;
- database server - a node on which the database is installed.

The diagram (Fig. 3) allows you to determine the requirements for the system and describe the functionality. It also helps to identify internal and external factors that affect the system and need further consideration.

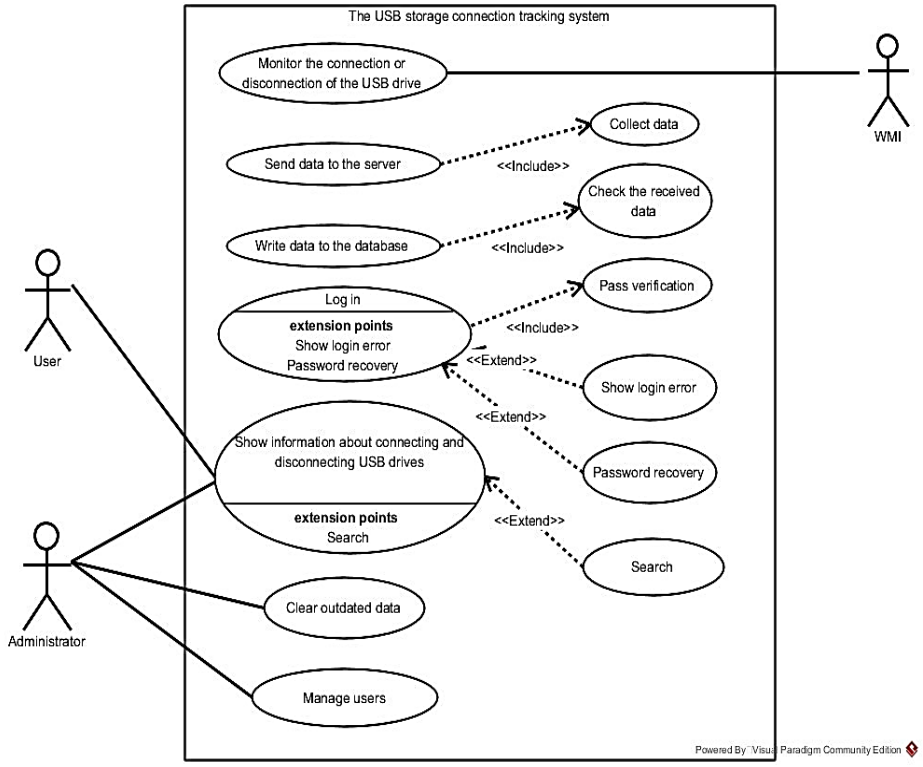

Fig. 3. - Diagram of usage options

Figure 4 shows the activity diagram, the main purpose of which is to track and save events that occur each time you connect or disconnect USB drives to computers for further analysis. This activity is carried out with the help of two services. The first service is installed on the computer that will be monitored. The actions performed by the client service are displayed on the "Client service" track. The second service is installed on the server. The actions performed by the server service are displayed on the "Server service" track.

4 Description of the software implementation of the system for monitoring the connections of USB-devices

To develop a system for monitoring USB device connections, the following were selected: C # and Python programming languages, technologies for creating HTML web interest, CSS and JavaScript, and PostgreSQL database.

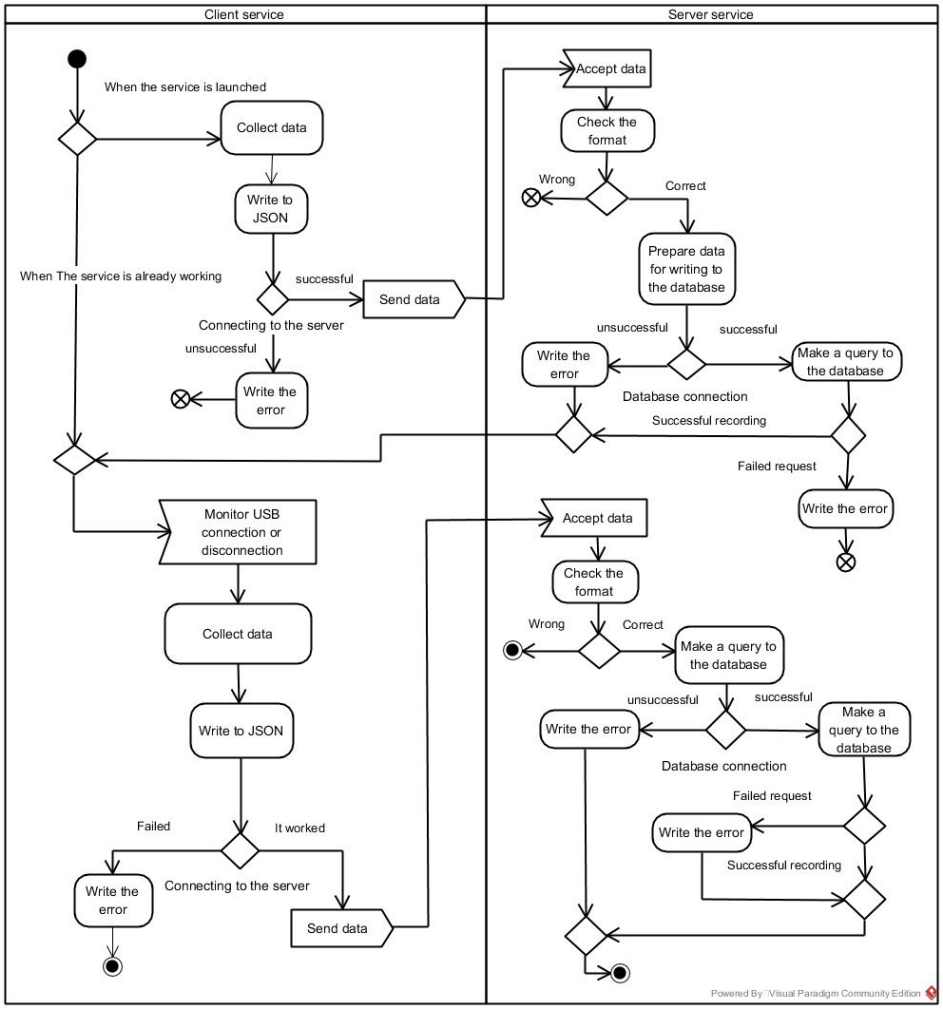

Fig. 4. Diagram of services

The part of the system that monitors USB device connection events must be implemented as a Windows service. Services implement the .NET Framework created by Microsoft to implement Windows. This platform allows you to run applications on the Windows operating system written in languages such as C # or VisualBasic.

Any monitoring system [5, 6, 7, 8, 9, 10, 11] must provide a convenient view of the information. In our case, this function will be performed by a web application. Python programming language is used to implement the backend. One of the needs of the system is to store events. Hence -the need to choose a database. PostgreSQL was chosen to implement this project. With the help of a web application, it is possible to

conveniently view and analyze events that have occurred on corporate computers. The application backend is based on the Flask micro framework.

The system was checked according to the plan (Table 3).

Table 3 - Verification plan

TC_ID	Verification requirements
TC1	Test the ability to register the client service and server service in the system using the installer
TC2	Test the ability to track the connection or disconnection of USB drives to a PC, send the received data to a server and store it in a database
TC3	Test the ability to configure network settings for client service and server service, the ability to run services on separate computers, the ability to view received events using a web application
TC4	Test the ability of authorized access to the system
TC5	Test the ability to reset the user password
TC6	Check for shared functionality
TC7	Test the ability to delete events and nodes
TC8	Test the ability to search
TC9	Test the ability to create and delete users

Figure 5 shows a fragment of the main page of the web application of the monitoring system. This page contains information about the computers that are being monitored, their IP/Mac-addresses, the total number of the events, the last date of the event, and the last time of the event.

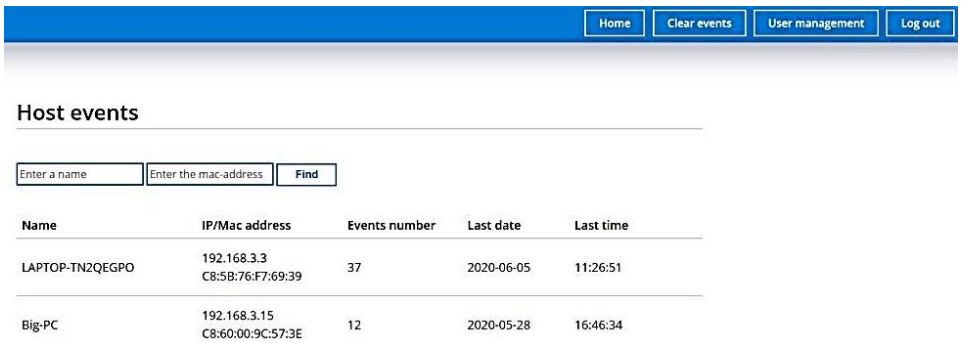

Fig. 5. - The main page of the web application

Once the USB device is connected, the data is added to the database. This means that the USB device connection event was successfully tracked, transferred to the server, and recorded to the database (Figure 6).

	userpc character varying (255)	id integer	eventdate date	eventtime time without time zone	vid character varying (255)
1	LAPTOP-TN2QEGPO	3	2020-05-28	13:34:47	0951

Fig. 6. - Created record in the database (fragment)

A convenient search allows you to track the connection with the specified parameters (Fig. 7).

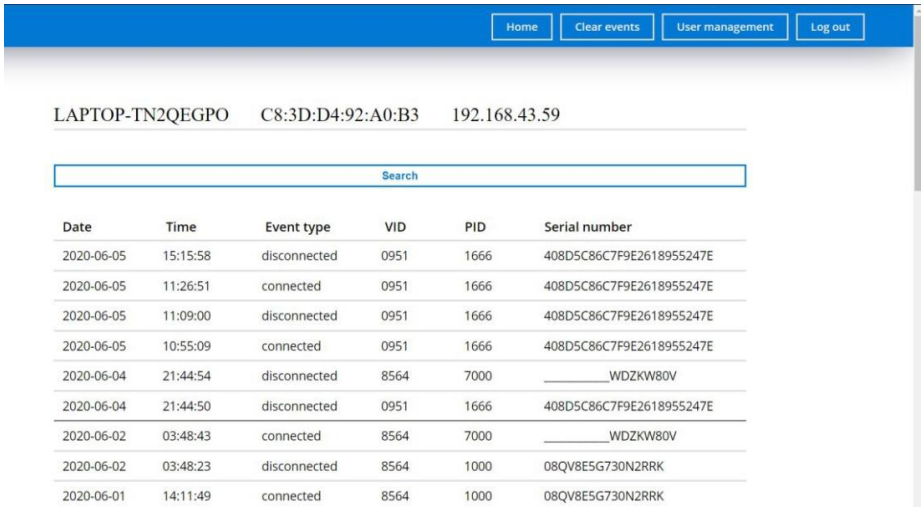

Fig. 7. - Found events

Testing the program according to a defined plan proved the efficiency of the developed system.

5 Discussion

The developed system allows you to supplement cybersecurity measures with a convenient tool for monitoring events. The software allows you to track connection events on corporate computers; provide centralized collection and storage of events for further analysis; have an intuitive web interface for easy viewing and analysis of events; provide the ability to search for the desired events.

The disadvantages that will be eliminated in the future include the impossibility:

- work with ActiveDirectory;
- identify the user account during which the device was connected;

– automatically determine the type and name of the company-manufacturer of the USB-device;
– remote complete blocking of USB-devices connection;
– creation of "white" lists of devices allowed for use in the corporate network;
– remotely delete USB device entries from the registry of the remote computer.

6 Conclusions

The following main results were received in this paper:

– The main tasks of modern information and/or cybersecurity systems and technologies to ensure information protection have been considered;
– A review of software for monitoring the connection of USB-devices revealed the urgency of developing a system that can be used by small companies to reduce the response time to leaks and increase the chances of establishing the identity of the infringer.
– The system is implemented in the form of two Windows services, utilities for configuring settings for running services and a web application.
– The performed efficiency test made it possible to recommend this software tool for monitoring USB-device connections.
– Further research will be aimed at integrating the developed monitoring system with the information security management system, which will allow to comprehensively solve the cybersecurity problem.

References

1. Meckl, S., Tecuci, G., Marcu, D., & Boicu, M. (2018). Integrating Collaborative Cognitive Assistants Into Cybersecurity Operations Centers. In AAAI Fall Symposium: ALEC (pp. 28-35).
2. Vielberth, M. & Pernul, G. (2018). A security information and event management pattern. https://epub.uni-regensburg.de/41139/
3. Nicolett, M. & Kavanagh, K. M. (2011). Magic quadrant for security information and event management. Gartner RAS Core Reasearch Note (May 2009).
4. Novikova, E. S., Bekeneva, Y. A., & Shorov, A. V. (2017, September). Towards visual analytics tasks for the security information and event management. In 2017 International Conference" Quality Management, Transport and Information Security, Information Technologies"(IT&QM&IS) (pp. 90-93). IEEE.
5. Lavrov E. Mathematical models for the distribution of functions between the operators of the computer-integrated flexible manufacturing systems / Lavrov, E., Pasko, N., Krivodub, A., Tolbatov, A. / 2016 Modern Problems of Radio Engineering, Telecommunications and Computer Science, Proceedings of the 13th International Conference on TCSET 2016 – Lviv-Slavske, 2016. – P. 72–75.
6. Tolbatov A. Data representing and processing in expert information system of professional activity analysis / Zaritskiy, O., Pavlenko, P., Tolbatov, A. / 2016 Modern Problems of Radio Engineering, Telecommunications and Computer Science, Proceedings of the 13th International Conference on TCSET 2016 – Lviv-Slavske, 2016. – P. 831–833.

7. Lavrov E. Cybersecurity of distributed information systems. The minimization of damage caused by errors of operators during group activity / Lavrov, E., Tolbatov, A., Pasko, N., Tolbatov, V. / 2017 2nd International Conference on Advanced Information and Communication Technologies, AICT 2017 – Proceedings – Lviv, 2017. – P. 83–87.
8. Lavrov E., Tolbatov, A., Pasko, N., Tolbatov, V. Ergonomic reserves for improving reliability of data processing in distributed banking systems. International Conference on Advanced Information and Communication Technologies. Lviv, 2017. P. 79–82.
9. Zaritskry, O., and et. al. Theoretical bases, methods and technologies of development of the professional activity analytical estimation intellectual systems. International Conference on Advanced Information and Communication Technologies. 2017. P. 101-104.
10. Gnatyuk S., N. Barchenko, O. Azarenko, A. Tolbatov, V.Obodiak, V.Tolbatov Ergonomic Support for Decision-Making Management of the Chief Information Security Officer. 1st International Conference on Cyber Hygiene and Conflict Management in Global Information Networks (CyberConf 2019) Lviv, November 29, 2019. P. 459-471.
11. Tolbatov A.V., Tolbatov V.A. Development concept modeling of business processes of modern industrial enterprises in terms of theoretical and legal approaches to the analysis information security. International scientific-technical magazine Measuring and computing devicesin technological processes. 2017. №1. P.196–199.
12. S. Gnatyuk, Critical Aviation Information Systems Cybersecurity, Meeting Security Challenges Through Data Analytics and Decision Support, NATO Science for Peace and Security Series, D: Information and Communication Security. IOS Press Ebooks, Vol.47, №3, pp. 308-316, 2016.
13. S. Gnatyuk, A. Okhrimenko, M. Kovtun, T. Gancarczyk, V. Karpinskyi, Method of Algorithm Building for Modular Reducing by Irreducible Polynomial, Proceedings of the 16th International Conference on Control, Automation and Systems, Oct. 16-19, Gyeongju, Korea, 2016, pp. 1476-1479.
14. Hu Z., Gnatyuk S., Kovtun M., Seilova N. Method of searching birationally equivalent Edwards curves over binary fields, Advances in Intelligent Systems and Computing, Vol. 754, pp. 309-319, 2019.
15. S. Gnatyuk, V. Kinzeryavyy, M. Iavich, D. Prysiazhnyi, Kh. Yubuzova, High-Performance Reliable Block Encryption Algorithms Secured against Linear and Differential Cryptanalytic Attacks, CEUR Workshop Proceedings, Vol. 2104, pp. 657-668, 2018.
16. Gnatyuk S., Kinzeryavyy V., Kyrychenko K., Yubuzova Kh., Aleksander M., Odarchenko R. Secure Hash Function Constructing for Future Communication Systems and Networks, Advances in Intelligent Systems and Computing, Vol. 902, pp. 561-569, 2020.
17. Fedushko S., Shakhovska N., Syerov Yu. Verifying the medical specialty from user profile of online community for health-related advices. CEUR Workshop Proceedings. Vol. 2255: IDDM 2018, Lviv, Ukraine, November 28–30, 2018. P. 301–310 (2018).
18. R. Odarchenko, V. Gnatyuk, S. Gnatyuk, A. Abakumova, Security Key Indicators Assessment for Modern Cellular Networks, Proceedings of the 2018 IEEE First International Conference on System Analysis & Intelligent Computing (SAIC), Kyiv, Ukraine, October 8-12, 2018, pp. 1-7.
19. Z. Hassan, R. Odarchenko, S. Gnatyuk, A. Zaman, M. Shah, Detection of Distributed Denial of Service Attacks Using Snort Rules in Cloud Computing & Remote Control Systems, Proceedings of the 2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control, October 16-18, 2018. Kyiv, Ukraine, pp. 283-288.