Development of OLAP Based Decision Support System for Information Security Monitoring at National, Regional and Corporate Levels

Konul Dashdamirova
Institute of Information Technologies, B.Vahabzade str., 9A, Baku, Azerbaijan Republic

Abstract
In the conditions where cyber threats are widespread and unavoidable, it is necessary to promptly detect cyber threats and quickly react to possible incidents in order to ensure the information security of the national information environment. In the article, the need for continuous monitoring of computer networks to ensure information security is highlighted. The main components of the process of ensuring information security at the national, regional and corporate levels are studied. Sources of data for information security monitoring, methods of collecting data from various sources are investigated, categories of Information Security Monitoring Systems (ISMS) are studied. The carriers of social dangers are always people or social groups. The peculiarity of social threats is that they always threaten a large number of people, even if they are directed specifically against one person.

Keywords
Information Security, Information Security Monitoring, SIEM, UBA, OLAP, Data warehouse

1. Introduction

Currently, about 5 billion users use the Internet, the largest and most complex information network in the world. The Internet network provides users with numerous information and communication technologies, information sources, e-commerce and entertainment sites [1]. Every year, the bulk of the community integrates into the internet, and the number of users increases dramatically. As the internet environment is rich in content for all ages, increasingly, people are becoming dependent on social networks, mobile phones, telecommunications, games and various cloud services. The increase in the number of the Internet users leads to an increase in the volume of information exchange, the creation of "Big Data", as well as the proliferation of harmful information and actions that can damage the psychological health and property of people. Factors such as the abundance of information, the age limit and religious-ethnic composition of users, the possibility of influencing the psychology of the masses, and others make cyberspace attractive for criminals [2]. Although the world countries pay great attention to the information security issues, the number of computer attacks increases every year, and new attack tools and methods appear. Hackers can carry out large-scale attacks anywhere in the world for various reasons. The number of cyber crimes such as cyber terrorism, identity theft, fraud is increasing rapidly. The number of cyber threats targeting the vital interests of the individual, society and the state is increasing. The opportunities brought by the Internet in some cases allow cyber threats to go beyond the individual or local level and become regional, national, continental or global in nature. At this time, the social security problems become urgent. Social threats are unfavorable processes and events occurring among people in society, which threaten people's life and health, their property, rights and legal interests.

13th International Scientific and Practical Conference from Programming UkrPROGP'2022, October 11-12, 2022, Kyiv, Ukraine
EMAIL: konulahmed@gmail.com (A. 1)
ORCID: 0000-0003-0365-6139 (A. 1)

The carriers of social dangers are always people or social groups. The peculiarity of social threats is that they always threaten a large number of people, even if they are directed specifically against one person. In order to prevent and eliminate such threats, by analyzing the parameters characterizing the social threat, the scale of the threat (local, regional, national, transnational), the area it covers (village, district, settlement, city, country) and the age group (0-6, 7-17, 18-30, 31-55, 56-61 and above), we should determine the duration of the danger, whether it is intentional or accidental, and so on.

Various security tools and methods are used to ensure information security in cyberspace, to detect and assess security incidents. Monitoring of information security in cyberspace is carried out in order to reliably organize the work of computer networks (CN), protect the completeness, confidentiality and accessibility of data. Information security monitoring (ISM) can serve to detect social threats, determine the nature of threats, attack targets, assess the state of information security within an organization, region, country, etc., as well as prevent cyber attacks in the future [3].

This research, the main components of the process of ensuring information security at the national, regional and corporate levels, and proposes a hierarchical structure for evaluating the data analyzed through ISMS. The sources and data collection methods on which ISMS are based are also considered. In order to provide support to decision-makers and improve analytical activity in this field, it proposes to develop a decision support system in ISMS.

2. The main components of the process of ensuring information security at the national, regional and corporate levels

Information security has become one of the main components of national security in cyberspace in conditions of increasing potential events, conditions, actions or processes aimed at harming the interests of the individual, society and the state [4]. National security is a set of officially adopted views to ensure the protection of the individual, society and the state from external and internal threats, threats of a political, economic, social, military, environmental and other nature. Ensuring national security is considered the duty of the government. The problems of monitoring the information space at the national, regional and corporate levels for the protection of the material and moral values of society from external and internal threats, the detection and prevention of social threats are becoming relevant. Approaches to information security are changing in a situation where various fields of activity are digitized, threats and attacks against digital systems are increasing. Security centers are created on the basis of monitoring systems, changes related to cyber security are made in the legislative framework, new laws and strategies are developed. Figure 1 shows the sequence of the ensuring process of information security at the national, regional and corporate levels (Figure 1).

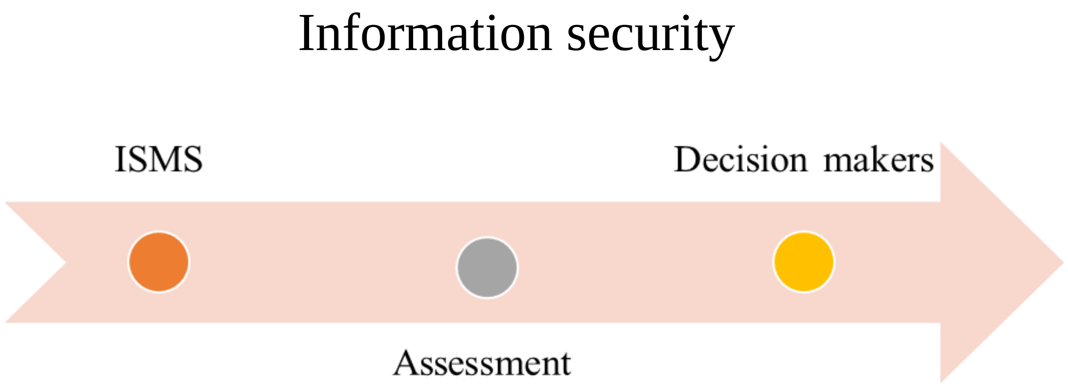

Figure 1: The main components of the process of ensuring information security

First of all, to monitor the national information space and determine the state of information security is necessary. The area covered by the danger, the scale of the danger, the targets of the attack, the time of continuation, the origin of the danger (intentional or accidental) and so on should be determined. For this purpose, the process of monitoring the information security of computer networks, collecting and analyzing information about security incidents in cyberspace is carried out. ISM is the process of collecting, systematizing and analyzing information about the state of the network and the behavior of users.

The purpose of this process is to identify information security breaches and gaps in the computer systems of the protected facility. ISMS automate the process of collecting and analyzing information about security incidents from various sources. Modern ISMS work in continuous, automatic mode, allow timely detection of threats, preparation of appropriate notifications and timely prevention of security risks (Figure 2) [5].

The main components of ISMS include software-technical, documentation and personnel part:

- The software-technical part includes tools for monitoring security events of the SIEM (Security Information and Event Management) class. Data collection from various sources is carried out through monitoring agents. Such sources can be information security tools (antivirus systems, security scanners, etc.), system and application software, CERT, etc. Information about security events is collected in the event server and ensures centralized processing of the system. Data processing is carried out in accordance with the rules established by the security administrator. The results of system activity and data received from agents are stored in the database. The system management console allows you to review the results of the system's work in real time and manage its parameters.
- The documentation part of ISMS includes a set of documents that describe the basic processes involved in identifying and responding to security incidents.
- The personnel part envisages employees responsible for working with ISMS.

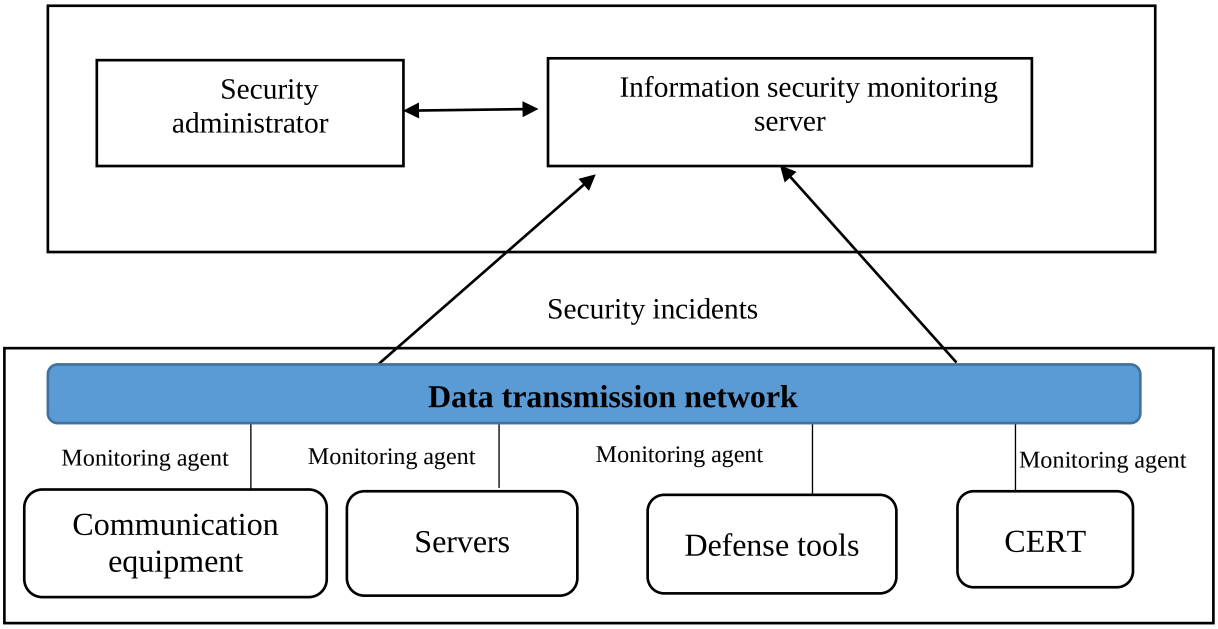

Figure 2: The structure of the ISMS

The next step for ensuring the security of the national information environment is the evaluation of the results obtained through ISMS at different levels (corporate, regional, national) within a country. Evaluation can be organized hierarchically, starting from the corporate level to regional and national levels (Figure 3). After evaluating the analyzed information within the framework of individual enterprise, organization, administration, the situation of information security within the framework of a village, settlement, district, city, and finally the region is evaluated accordingly. In the last stage, on the bases of the regional level, we can assess the level of information security at the level of a country.

Cluster analysis methods, expert assessment methods, multi-criteria assessment, multidimensional assessment methods can be used to evaluate the results of information security monitoring. Assessment of the results of information security monitoring allows you to quickly analyze the current situation in the field of information security, detect signs of information security incidents.

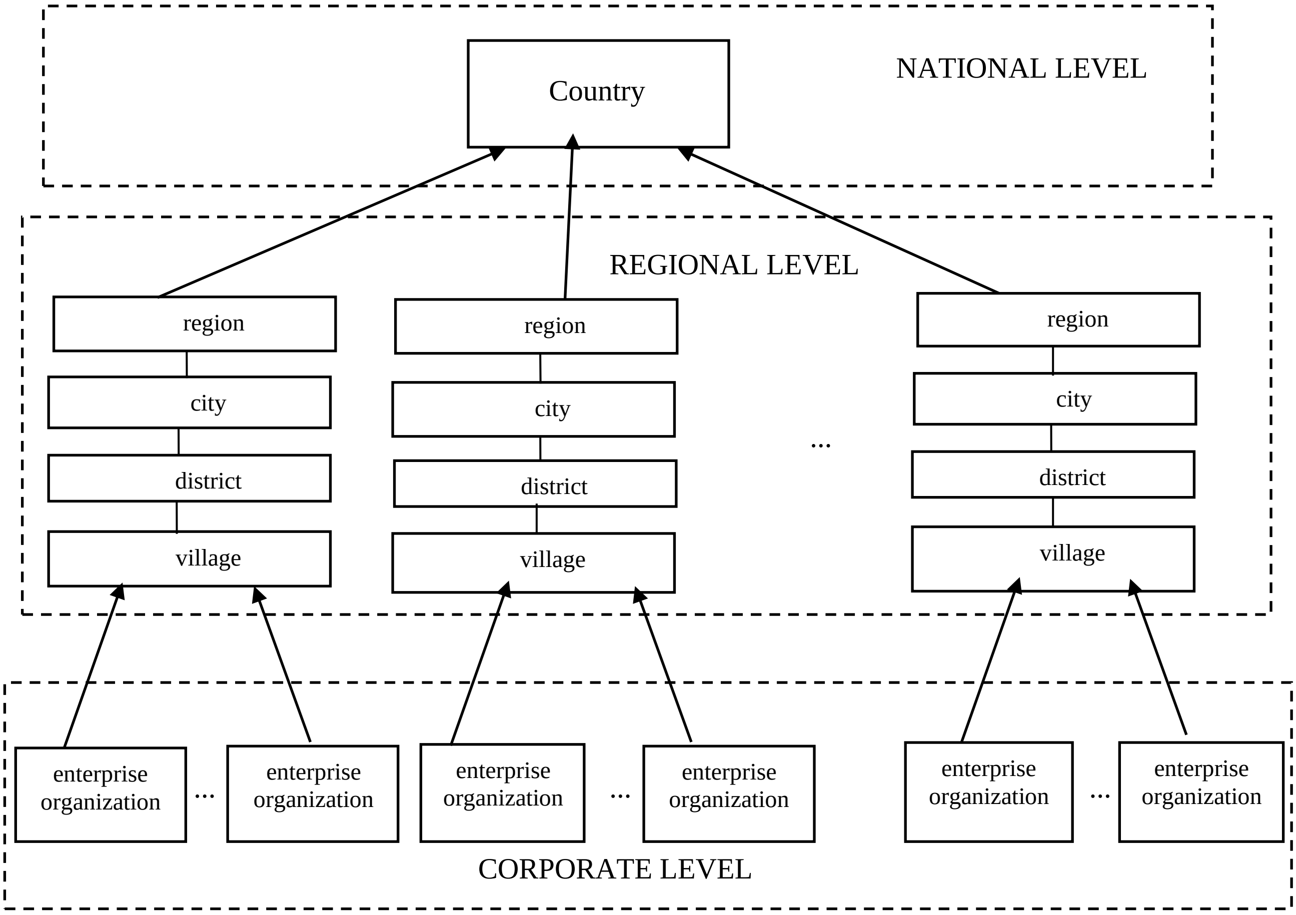

Figure 3: Hierarchical assessment of the results of the analysis at the corporate, regional and national level

Based on the results of monitoring, we can assess the current state of information security at the level of a country and make predictions about its future state and give recommendations to decision-makers.

3. Analysis of sources on which ISMS are based

Information security is monitored by the process of checking all security incidents obtained from various sources. The source of incidents can be CERTs, antivirus systems located in the infrastructure of various organizations, operating system logs, scanners for security analysis of information infrastructure, network equipment, and other sources (Figure 4) [5].

CERT (Computer Emergency Response Team) is a group of computer security experts involved in collecting, monitoring, classifying, and neutralizing incident information. The main purpose of CERT is to analyze incidents sent by users (phishing, social engineering), suspicious files, viruses, as well as network traffic sessions, to respond quickly to new threats, inform users and develop security recommendations [6].

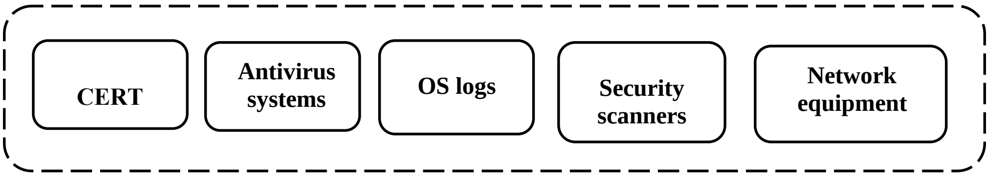

Figure 4: Sources for ISM

The first CERT group was formed at Carnegie Mellon University in 1988 after thousands of servers were infected with the Morris worm. The group currently has the status of a CERT coordination center and licenses and coordinates the activities of information security incident response centers around the world. National, regional or industrial CERTs can be established in coordination with Carnegie Mellon University. Currently, many companies around the world also create CERTs, but not all of them receive official status [7]. In total, there exist currently about 250 CERT teams in various countries around the world. Analysis of data collected in CERTs can allow for the timely detection and prevention of cyber threats and the assessment of the level of information security within a country to ensure the social security of society.

Today, computer viruses and malware are a real source of danger for any enterprise, organization, and others that use information technology in their activities. The widespread use of these global networks can be explained by the insufficient attention to network security issues in a large number of local computer networks. Computers are increasingly infected with malicious software when working with Internet resources or through email messages. The target of viruses can be any user's computer, global or local computer networks. The damage can lead to the failure of the computer and all computer networks in general, the violation of data integrity, accessibility, and confidentiality.

Every year, the creation of new types of viruses that can bypass traditional protection methods raises the issue of protecting computer networks from malware. An important way to fight computer viruses is to prevent them in time. Timely detection of infected files or disks, and complete destruction of detected viruses on each computer help to prevent the spread of the virus epidemic to other computers and computer networks. Antivirus software is a special program that is used to detect computer viruses, as well as undesirable (considered harmful) programs, recover infected (modified) files by these programs, and prevent infection (modification) of files or operating systems with malicious code. Network antivirus programs carry out monitoring of servers, network computers, and installed software, allow you to monitor e-mail, data of allowed network protocols (HTTP, FTP), file servers, external carriers (floppy disks, flashcards, CDs, DVDs), as well as all channels through which computer viruses and malicious programs can penetrate [8].

The essence of the antivirus monitoring method is that the antivirus program is constantly in the computer's memory and monitors all suspicious actions performed by other programs. Antivirus monitoring allows you to check all running programs, created, opened, and saved documents, programs, and files received via the Internet. The antivirus monitor will inform the user if any program tries to perform potentially dangerous actions.

Log files found in the logs of operating systems or web servers contain system information about the operation of the server or computer and information about the user behavior. The purpose of log files is to record all operations performed on the webserver or computer for monitoring by the administrator. This information is of great importance in the event of security incidents. Regular monitoring of logs and analysis of log files allows to identify errors in the operation of a particular system or site, diagnose malicious activity, identify threats, threats, collect information about user behavior, as well as evaluate according to various criteria [9].

Weaknesses in information systems, infrastructure nodes, and elements of the information security complex create great problems for information security. To identify vulnerabilities, companies need to analyze the security of their information infrastructure. As a rule, vulnerability scanners are used for security analysis from automatic instruments operating in static and dynamic scanning modes. At present, this class of tools allows you to solve a wide range of problems. A vulnerability scanner is a program that identifies and creates a registry of all systems connected to the network (servers, computers, virtual machines, containers, firewalls, switches, and printers). The program allows you to identify each device, the operating system and installed programs on this device, as well as other attributes such as open ports and user accounts and passwords, as well as track other elements that pose a potential threat to information security [10].

Faults in the hardware or software of the CN, slowing down or stopping the operation of important network services can lead to unpleasant consequences. A modern network equipment monitoring system is a complex information system that monitors servers, hosting, processes, and services on users' computers, as well as files, folders, and databases. It consists of the following components.

- network device indicators (CPU, temperature, device availability, packet loss, interface errors, available throughput, etc.) are critical parameters that need to be monitored;
- monitoring – the process of collecting, assembling, and analyzing indicators to improve the understanding of the characteristics and behavior of the components of the system. The data collected as a result of the monitoring can be visualized and drawn in the form of various graphs, diagrams, and histograms.
- the warning system is an important component that takes action when changes occur in the values of the observed indicators. When the critical value is reached, the metric value can try to solve the problem itself according to the developed scenario or send an alert to the responsible person using SMS, email, and so on.

The network equipment monitoring system allows receiving timely information about the fault, controlling the situation, to eliminate the fault with minimal time loss [11]. During ISM, the monitoring information can be collected from various sources using both automated and non-automated tools. Primary data collection is used to analyze the state of information security and conduct various types of assessments. The following methods can be applied to obtain primary data during the use of automated monitoring tools (Figure 5):

- agent-based data collection (agents for security incident monitoring);
- data collection without agent;
- questionnaires (forms);
- software.

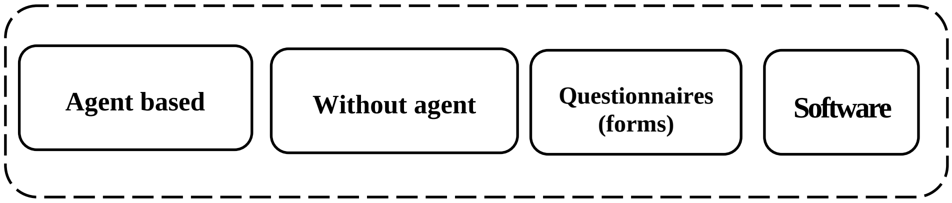

Figure 5:. Methods for collecting information from different sources

A security monitoring agent is software installed on information infrastructure components and information system nodes to gather the necessary information directly from a source. Monitoring agents can be used to collect information on security incidents, software effectiveness, user behavior, and other information.

The method of collecting data without agents involves the receipt of data from sources over the network without installing additional software for monitoring. Non-Agent data collection methods include:

- Read data directly from security log files or databases;
- Receiving information from sources using standard protocols for transmitting information about security events;
- Data collection by connecting to the program interface or the web service of the data source.

By the usage of agent-free data collection method, data collection can be carried out about security incidents, the operability of the software, and other information that the source can provide.

The collection of data on security incidents using questionnaires (forms) is carried out by filling in special electronic (paper) forms and then transferring them to information security monitoring personnel.

Data collection method using software includes information management systems on information security threats, security control systems, inventory means of software and technical means, software and information protection tools, and so on [12].

4. Categories of ISMS

All currently established and used ISMS can fall into one of the following categories.

SIEM is a system that allows analyzing data obtained from various sources in real-time. SIEM is a combination of Information Security Management and security event management systems into a single security management system. The results of the analysis carried out by SIEM are presented in a single interface, accessible to security analysts. This also facilitates the study of the corresponding characteristic features of security events and allows analyzing the events that occur in order to respond to security threats in real-time (Figure 6). Sources of information for SIEM systems can be antivirus programs, authorization and authentication systems, network screens, security walls, logs of network equipment, servers and workstations, intrusion detection and prevention systems (IDS / IPS), information leakage prevention systems (DLP) and other programs [13].

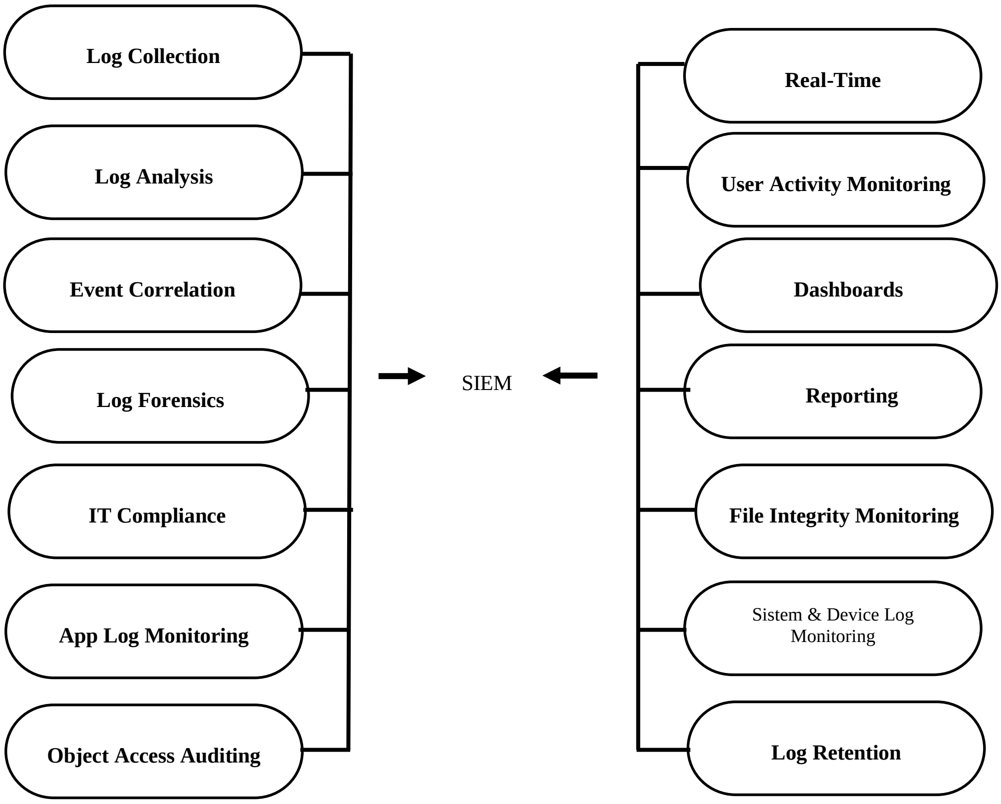

Figure 6: Security Information and Event Management

UBA (User Behavioral Analytics) – systems that collect and analyze all behaviors, including managed data, used to manage fraudulent activities at the expense of financial threats with internal threats [14].

UEBA (User and Entity Behavioral Analytics) – systems aimed at searching for and detecting anomalies in the behavior of users and various systems. A class of behavioral analysis systems has been established because companies use many different data collection systems to ensure information security. At the same time, employees are not always able to review all the information received and respond to potential events in a timely manner. UEBA systems increase efficiency by compiling profiles and ensuring timely response to possible data leaks [15].

Employee monitoring and time recording systems are systems that allow the organization to analyze the activities of employees and monitor the use of working time in the workplace, as well as control business processes, solve several tasks related to confidential information leaks, and further investigate of incidents [16].

Different types of attack detection and detection systems are aimed at improving the overall protection of the corporate network [14].

5. The architecture of the decision support system in ISMS

To ensure the efficiency of decision-making is necessary in order to quickly respond to security breaches and incidents in information security monitoring systems. In order to support decision-makers and improve analytical activities in this area, the development of a system that supports decision-making in information security monitoring systems is proposed.

A decision support system is a computer system that allows decision-makers to make more reasonable and correct decisions based on analytical recommendations provided to them. The decision support system can be created on the basis of various technologies, including OLAP (Online Analytical Processing) and Data Warehouse (DW) (Figure 7) [17]. The OLAP concept was described in 1993 by Edgar Codd, a well-known database researcher and author of the relational data model. OLAP is a key component of the database. This is a technology that collects, stores, and analyzes multidimensional data. Performs multidimensional, operational, and analytical data processing in real-time. For the preparation of reports, the construction of forecast scenarios, and statistical calculations based on large information systems with a complex structure are intended [18]. Through OLAP technology, the original data is converted into information that can be used for decision-making. We can visualize the results of the analysis and present the data in the form of graphs.

A warehouse is a place where all analytical information is collected for decision-making. ETL (Extract, Transform, Load) is a three-step process called extraction, conversion, and loading that collects data from multiple sources in a single parent repository.

- Extraction - extraction of data from external sources in an understandable format;
- Transformation - the conversion of primary data into suitable structures for the establishment of an analytical system;
- Loading - uploading data to the warehouse. ETL processing is usually done by software, but can also be done manually by system operators. Unnecessary data is cleaned up on the basis of statistical or expert methods [19].

Figure 7 presents the architectural-technological model of the decision support system for ISMS.

At the first level, data sources are identified for ISM. The source of the data can be CERTs created within an organization, a region, a country, network antiviruses, OS logs, security scanners, network equipment, and so on.

At the second level, the process of collecting primary data from various sources should be carried out for the ISM system. Data can be collected from sources within an organization, a region, or a country. Data collection can be done with agent programs, without agents, questionnaires (paper or electronic), or software. To ensure the high quality of the data before it falls into a single Database, this may be necessary to clean it and delete unnecessary data. Therefore, in the intermediate stage, during the transition to the third level, the data enters the field of data purification, and the ETL process is carried out as an intermediate stage.

Depending on the issue set at the third level, data on security incidents collected from sources within an organization, region, or country by means of data collection methods (one or some of them may be) is collected in the form of a separate database (DB) in one DW. Based on the data collected in each DB, reports are prepared for analysis using OLAP technology.

On the fourth level, reports prepared for analysis on the basis of a separate database are collected in DW. OLAP technology prepares reports for analysis by decision-makers on surveys sent to the data warehouse.

Analysis of security incidents collected from different sources within one organization, one region, or one country allow to determine and assess the state of information security within an organization, one region, or one country, and to identify the sources of threats.

6. Conclusion and Future Scope

The rapid development of the global Internet and ICT, and the impact on all areas of human activity, raises the information security problems. In the article, the main components of the process of ensuring information security at the national, regional and corporate levels were studied. ISMS were analyzed for the purpose of prompt detection of cyber threats and quick response to possible incidents. A hierarchical structure was proposed to evaluate the results of information security monitoring. Sources of primary data for İSMS were investigated, and categories of İSMS were analyzed. As a result of the analysis, to ensure the speed of decision-making for rapid response to security breaches and incidents was determined. For this purpose, the architectural-technological model of the decision support system based on OLAP technologies and database was proposed to support decision-makers.

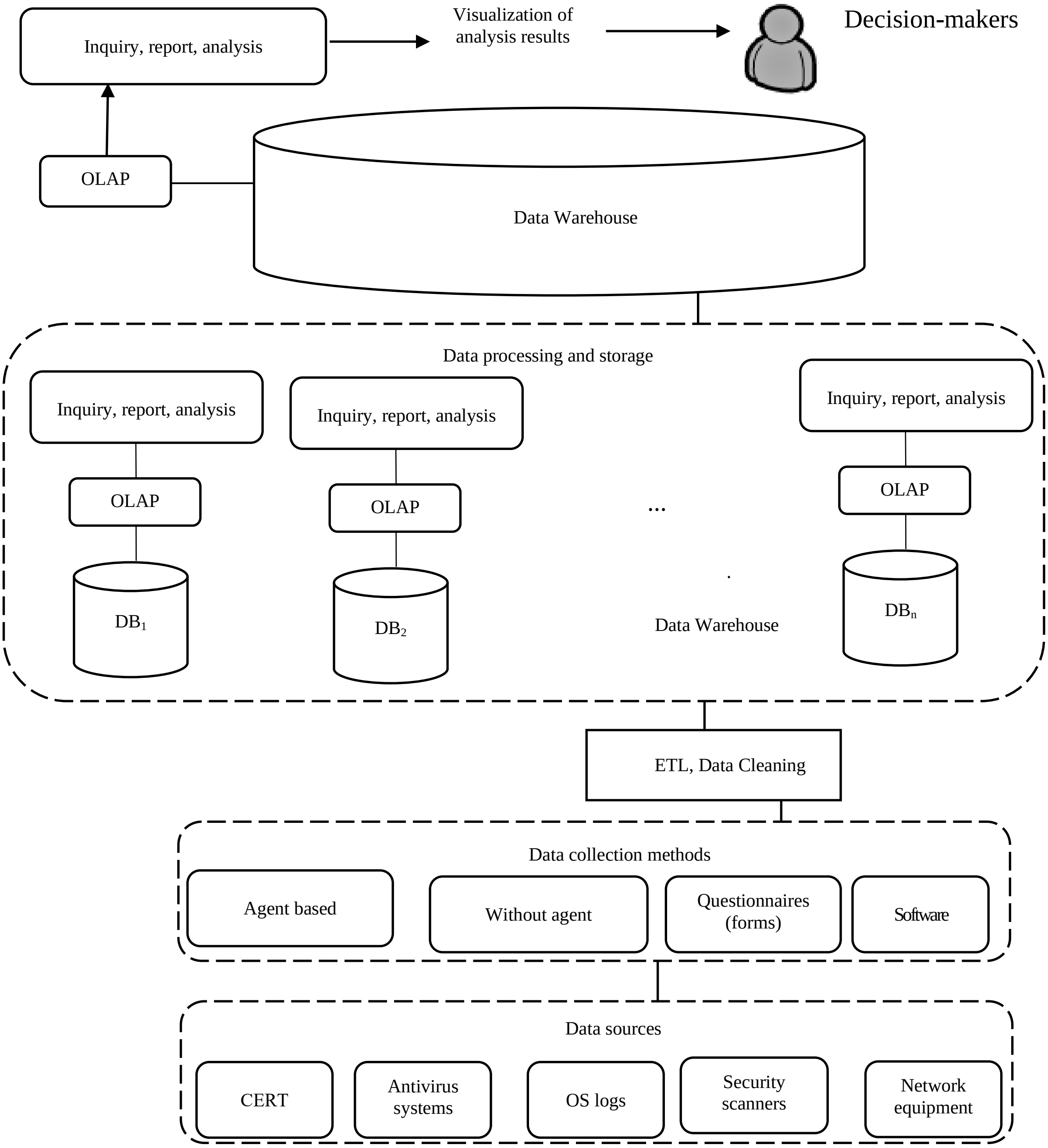

Figure 7: Architectural-technological model of Decision Support System for ISMS

7. References

[1] Special report - DIGITAL 2021, URL: https://wearesocial.com/uk/blog/2021/01/digital-2021-uk/

[2] R.S. Mahmudova, K.Q. Dashdamirova Analysis Of Information Security Problems In The Information Society Environment, Problems of Information Society, №2, 2021 pp.83-94. DOI : 10.25045/jpis.v12.i2.06

[3] Дашдамирова К. Г. Система поддержки принятия решений в области мониторинга информационной безопасности / XXI Международная научно-техническая конференция "Развитие информатизации и государственной системы научно-технической информации" (РИНТИ-2022), Минск, Беларусь, 2022, с. 95-99

[4] R.M. Alguliyev, Y. N. İmamverdiyev, R.Sh. Mahmudov. Information security as a national security component, Problems of Information Society, 2020, №1, p.3-25. DOI : 10.25045/jpis.v11.i1.01

[5] В. Сердюк, HP ArcSight - эффективный инструмент для мониторинга событий ИБ "InformationSecurity. Информационная безопасность" №1, 2013, с. 32-33.

[6] G. Littlewort et al. The computer expression recognition toolbox (CERT). IEEE International Conference on Automatic Face &amp; Gesture Recognition (FG). IEEE. 2011, P. 298-305.

[7] Software Engineering Institute. URL: https://www.sei.cmu.edu/about/divisions/cert/index.cfm

[8] Y. K. Yazov, S. V. Solovyov. Protection of information in information systems from unauthorized access. Kvarta. 2015, pp. 357-440.

[9] H. Barringer et al. Formal analysis of log files //Journal of aerospace computing, information, and communication. 2010. T. 7. №. 11. pp. 365-390. doi: 10.2514/1.49356

[10] H. Holm. Performance of automated network vulnerability scanning at remediating security issues. Computers &amp; Security. T. 3. No. 2. 2012, pp. 164-175.

[11] H. M. Cortes, P. E. Santos, J. I. da Silva Filho. Monitoring electrical systems data-network equipment by means of Fuzzy and Paraconsistent Annotated Logic //Expert Systems with Applications. 2022. T. 187. pp. 115865. doi.org/10.1016/j.eswa.2021.115865

[12] T. C. Lethbridge, S. E.Sim, J. Singer Studying software engineers: Data collection techniques for software field studies //Empirical software engineering. 2005.T. 10. №. 3. pp. 311-341.

[13] H. Karlzen An Analysis of Security Information and Event Management Systems-The Use or SIEMs for Log Collection, Management and Analysis : 2009.

[14] C. Bernaschina et al. A big data analysis framework for model-based web user behavior analytics //International Conference on Web Engineering. Springer, Cham, 2017. pp. 98-114.

[15] M. Shashanka, M. Y. Shen and J. Wang, User and entity behavior analytics for enterprise security, 2016 IEEE International Conference on Big Data (Big Data), 2016, pp. 1867-1874, doi: 10.1109/BigData.2016.7840805.

[16] L. Kufel. Security event monitoring in a distributed systems environment. IEEE security &amp; privacy. T. 11. No. 1. 2012, P. 36-43.

[17] E. F. Codd Providing Olap. On-line Analytical Processing to User-Analists: An IT Mandate. Associates, 1993. T. 19.

[18] J. Krzysztof. Data Mining: A Knowledge Discovery Approach. Springer. 2007, pp. 123.

[19] G. Nabibayova. About an application of OLAP-technology in decision making support systems. 5th International Conference on Application of Information and Communication Technologies (AICT). 2011, IEEE. pp. 1-4.