Ministry of Education and Science of Ukraine
Ternopil Ivan Puluj National Technical University

Computer Information Systems and Software Engineering
(full name of faculty)
Computer Science
(full name of department)

QUALIFYING PAPER

For the degree of

Bachelor
(degree name)

topic: Cybersecurity event management information system for creating firewall rules

Submitted by: fourth year student 4 , group ISN-42
specialty 122 «Computer Science»
(code and name of specialty)

		Njikonye Godswill Nwakanma
	(signature)	(surname and initials)
Supervisor		Zolotyi R.
	(signature)	(surname and initials)
Standards verified by		Matsiuk O.
	(signature)	(surname and initials)
Head of Department		Bodnarchuk I.
	(signature)	(surname and initials)
Reviewer		Stadnyk N.
	(signature)	(surname and initials)

Ternopil, 2022

Ministry of Education and Science of Ukraine
Ternopil Ivan Puluj National Technical University

Faculty Computer Information Systems and Software Engineering
(full name of faculty)

Department Computer Science
(full name of department)

APPROVED BY
Head of Department

(signature) (surname and initials)

« » 20___

ASSIGNMENT

for QUALIFYING PAPER

for the degree of Bachelor
(degree name)

specialty 122 «Computer Science»
(code and name of the specialty)

student Njikonye Godswill Nwakanma
(surname, name, patronymic)

1. Paper topic Cybersecurity event management information system for creating firewall rules

Paper supervisor Ph. D., Assoc. Prof., department Computer Sience, Roman Zolotyi
(surname, name, patronymic, scientific degree, academic rank)

Approved by university order as of «*17* » *12* 2021 № *4/7-1068*

2. Student's paper submission deadline 23.06.2022

3. Initial data for the paper Technical requiremen for patient card

4. Paper contents (list of issues to be developed)
Introduction,
CHAPTER 1
CHAPTER 2
CHAPTER 3
Conclusions

5. List of graphic material (with exact number of required drawings, slides)
1. Title page
2. Relevance of work
3. Main tasks of work
4. Main part (4-8 slides)
5. Conclusions

6. Advisors of paper chapters

Chapter	Advisor's surname, initials and position	Signature, date	
		assignment was given by	assignment was received by
Life safety, basics of labor protection	Ph.D. (Engineering), Assoc. Prof. department Valeriy Lazaryuk		

7. Date of receiving the assignment _____

TIME SCHEDULE

LN	Paper stages	Paper stages deadlines	Notes
1	Acquaintance with the assignment for the qualification work	24.01.2022	done
2	Analysis of literary sources	04.01.2022-30.01.2022	done
3	Justification of the relevance of the research	31.01.2022-06.02.2022	done
4	Analysis of the research subject and subject area	07.02.2022-13.02.2022	done
5	Design section 1	14.02.2022-06.03.2022	done
6	Design section 2, 3	07.03.2022-03.04.2022	done
7	Completion of the task for the unit "Life safety"	04.04.2022-17.04.2022	done
8	Completion of the task for the unit "Basics of labor protection"	18.04.2022-01.05.2022	done
9	Completion of qualification work	02.05.2022-15.05.2022	done
10	Standard control	16.05.2022-22.05.2022	done
11	Check for plagiarism	06.06.2022	done
12	Preliminary defense of qualifying work	07.06.2022	done
13	Protection of qualification work	6.07.2022	

Student _____ Njikonye Godswill Nwakanma
(signature) (surname and initials)

Paper supervisor _____ Roman Zolotyi
(signature) (surname and initials)

ABSTRACT

Cybersecurity event management information system for creating firewall rules // Qualification work of the educational level "Bachelor" // Njikonye Godswill Nwakanma // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Computer Science, group ISN-42 // Ternopil, 2022 // P. , Fig – , Table – .

Keywords: INFORMATION SYSTEM, CYBER SECURITY, FIREWALL, DEVELOPMENT, SOFTWARE MODULE.

In order to reach the goal, in the thesis work, a detailed information about the actuality of the development of the software module of the cybersecurity control system was reviewed, a selection of software and technical aids for the creation of the module was primed, and a test was carried out with virtual information systems.

The thesis presents a software module for automating the creation of rules for Firewall according to IDS indicators and rules defined by the security administrator. Keywords: IDS systems, cyber security, firewall, information systems, APT attacks, software module.

The purpose of the thesis is to develop a program module for managing cybersecurity events. In order to achieve the goal in the thesis, the general questions about the urgency of the development of the software module for the management of the events of cybersecurity are considered, the choice of software and technical means for the creation of the module is substantiated, as well as its testing in the virtual information system has been conducted.

In the thesis is presented a program automation module for creating rules for Firewall according to IDS indicators and rules defined by the security administrator.

LIST OF CONVENTIONAL SYMBOLS OF ABBREVIATIONS AND TERMS

SOC - Security Operations Center

SIEM - information security monitoring and management

CONTENT

INTRODUCTION

In the modern world, information systems have taken an important place in all areas of human activity and helped to move to a new level of development thanks to automation. There are no small things when it comes to ensuring security, and the secondary role of some of its components is assigned purely conditionally. However, many people have the impression that Firewall and antivirus software, if properly configured, can handle any threat. Unfortunately, this is not enough nowadays. Even computer systems with the most advanced protection cannot be called completely invulnerable. Most computer security experts agree that creating a completely secure system is impossible.

The complexity and number of various threats to information security is increasing every day, and the so-called targeted or long-term ART attacks, which have a complex implementation structure, are especially dangerous. At the same time, the number of systems designed to protect business from these types of attacks is also increasing. In these conditions, it becomes necessary to detect an information attack in a timely manner and take complex measures aimed at its localization and prevention.

As a result of the operation of such systems, administrators receive hundreds of thousands of messages from many different sensors every day. The functioning of each of the subsystems separately is critical for the business as a whole, so specialists are forced to analyze this entire flow of information to prevent attacks in the future. The subject of the thesis research

The object of research of the thesis is a real-time cyber protection system. Over the past 10 years, cyber attacks have developed significantly and changed their typical appearance and execution algorithm. Due to the widespread practice of using basic types of protection, such as antivirus and firewall, information systems have become less vulnerable to typical attacks, such as: virus attacks, DDOS attacks, ARP

spoofing, and so on, but APT attacks require more advanced means of combating , such as SIEM.

1 STATEMENT OF THE PROBLEM AND RELEVANCE

1.1 Basic terms

The subject of research of this work is the process of automating the formation of commands for IPS actuators for SIEM (system of event management and information security) in SOC (security operations center). Firewall acts as an IPS actuator in this work. To understand the place of SOC in the network, a structural diagram of a typical network of the organization is shown (fig 1.1).

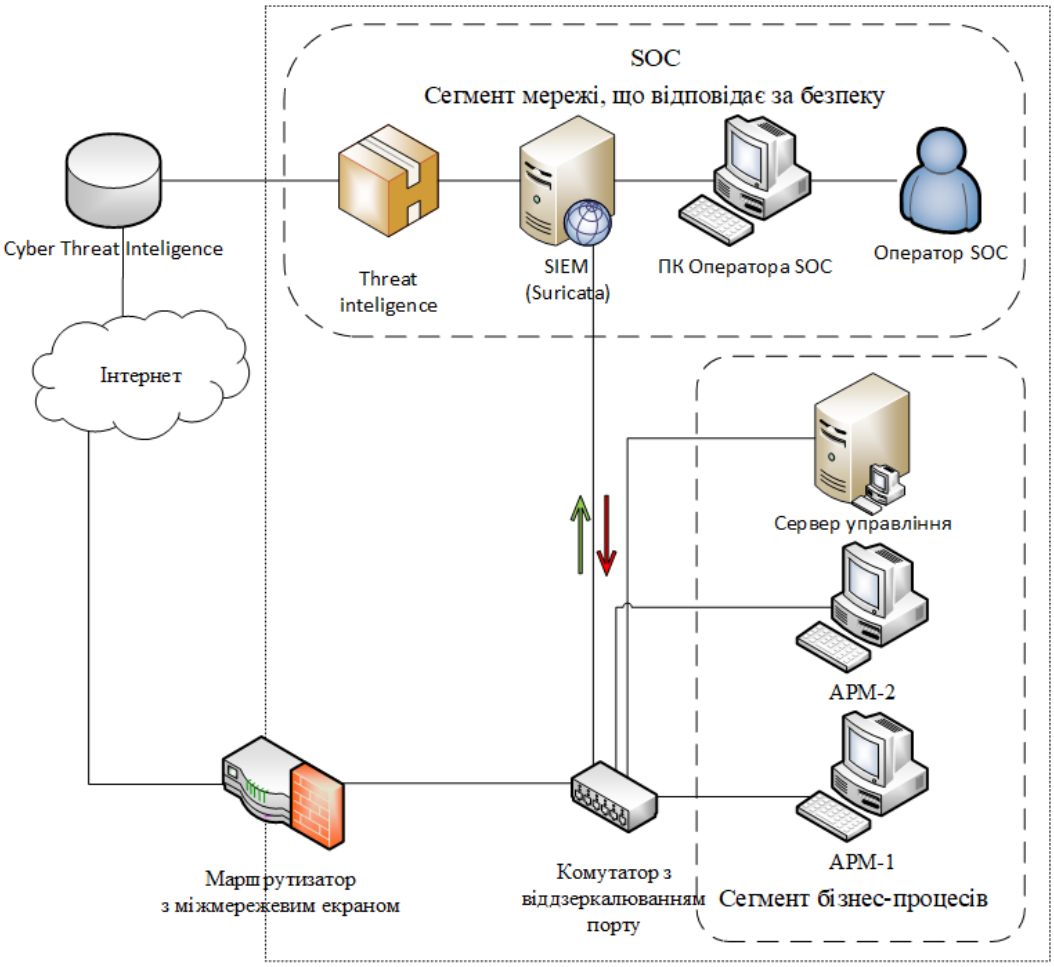

Figure 1.1 – Structural diagram of a virtual network.

The goal of the thesis is to develop a software module of the cyber security event management system, which will work in the middle of SIEM and analyze the collected data from IDS sensors, after which it will form commands for IPS

actuators. The result of the work should be a software module for automating the creation of access control lists based on IDS Suricata event logs..

Information system is an organizational and technical system in which information processing technology is implemented using technical and software tools. Telecommunications system - a set of technical and software tools designed for the exchange of information by transmitting, radiating or receiving it in the form of signals, signs, sounds, moving or still images or otherwise.

An information and telecommunication system is a set of information and telecommunication systems that act as a single entity in the process of processing information [1]. Automation is a stage of machine production, which is characterized by the transfer of the control function from a person to automatic devices [2]. Security analysis is a complex process performed by security analysts who have experience in identifying, determining and understanding indicators of potential threats in electronic logs (traces of computer systems).

Intrusion detection system – software or hardware designed to detect the facts of unauthorized access to the information network for the purpose of unauthorized remote management of it. By type, intrusion detection systems are divided into network, node and hybrid. SOC (Security Operations Center) is a security operations center, a centralized unit of the institution that solves information and cyber security issues at the organizational and technical level.

SIEM (Security Information and Management System) is a system for monitoring and managing information security. This is a category of software that provides organizations with actionable information about potential network security threats by analyzing data and prioritizing threats. This is possible thanks to the centralized analysis of security data provided by various systems, including antivirus programs, firewalls, IPS/IDS.

Ensuring information security is a set of measures designed to achieve a state of protection of the needs of individuals, society and the state in the processing, storage and dissemination of information. The state implements its measures through

relevant bodies, and citizens, public organizations and associations with relevant powers, in accordance with the legislation.

An exploit is a computer program, a piece of software code, or a sequence of commands that uses vulnerabilities in software and is designed to attack a computer system. The goal of an attack can be both to seize control over the system and to disrupt its functioning.

A DHCP server is a network protocol that allows computers to automatically obtain an IP address and other parameters necessary to work in a computer network using the TCP/IP protocol. For this, the computer turns to a special server called a DHCP server. A network administrator can specify a range of addresses that are distributed among computers. This avoids manual configuration of network computers and reduces the number of errors. The DHCP protocol is used in most large networks using TCP/IP technology.

APT attack is short for Advanced Persistent Threat (sophisticated persistent threat or targeted cyberattack), on the one hand, a sophisticated persistent threat is a highly accurate cyberattack. On the other hand, an APT can be called a hacking attack sponsored by a government, organization or person. Cybersecurity is the process of applying security measures to ensure the confidentiality, integrity and availability of data.

1.2The importance of information systems

During the rapid development of networks, information systems have taken one of the most important places in the work processes of organizations. Information systems are designed for timely provision and satisfaction of users' information needs. For example, in the activities of enterprises, there is a practice of creating and functioning of a single corporate information system that satisfies the information needs of all employees, services and divisions of the organization

The growing role of information systems in the field of military management leads to an increase in threats of the use of cyber means against the interests of Ukraine both from within the state and from abroad. At present, the capabilities of intrusion detection systems are a necessary criterion for the infrastructure of information protection in connection management systems and parts that use information systems connected to the global Internet.

Information systems can function both with the use of technical means and without such use. This is a question of economic feasibility. Depending on the degree of automation of information processes in the information system management system, they are classified into 3 categories: - manual information systems are characterized by the absence of modern technical means of information processing and the execution of all operations by a person. For example, about the activities of a manager in a company where there are no computers, it can be said that he works with a manual information system; automatic information systems perform all information processing operations without human participation; - automated information systems involve the participation of both humans and technical means in the information processing process, and the main role is assigned to the computer. The modern term "information system" necessarily includes system automation. Automated information systems, taking into account their wide use in the organization of management processes, have various modifications and can be classified, for example, by the nature of information use and by the field of application [2].

1.3 Types of network attacks on information systems

Let's consider several of the most dangerous types of network attacks. One of the quite common types of attacks is buffer overflow. This type of attack is often a component of various types of malicious attacks. "Overflow" attacks, in turn, have many varieties: attacks on the stack, on string formatting functions. The task of attacks on the stack is to overflow its buffer, by writing data (a set of symbols

overflows the stack and any instructions for the program) of a larger volume than was laid programmers As a result, the program, after overflowing the buffer, can execute the instructions written by the attacker in the stack. a string formatting attack also affects the stack, but involves replacing one address with another containing the attacker's commands.

"Passive" attacks using a sniffer are especially dangerous because they are difficult to detect and are made from a local network. "Passive" attacks help attackers to obtain such information directly from the network as: information about networks, traffic of SSL or TLS, TCP and UDP sessions, capture of IP or MAC addresses, numbers of used ports, user names, passwords.

APT attacks Targeted attacks (APT attacks) are attacks directed against specific commercial organizations or government agencies. As a rule, such attacks do not have a mass nature and are prepared for a rather long period. Criminals study the information systems of the object under attack, find out which software is used for certain purposes.

The objects of the attack are very specific information systems or people. Malicious software is specially developed for the attack, so that standard antivirus and protection tools used by the object and well-studied by the attackers cannot detect the threat. Most often, these are zero-day vulnerabilities. An APT attack consists of the following stages:

network research - the stage includes drawing up a network map, recording the IP addresses of servers, routers, switches, DNS servers, searching for VPN tunnels, honeypots, proxies, etc.;

search for vulnerabilities - the stage includes the search for vulnerabilities on servers, routers, etc.;

exploitation of vulnerabilities – attackers hack a server, router or other computer equipment located in the network or subnet of the target machine;

hacking of employee accounts - is mainly carried out for phishing, relevant for collecting information, logins and passwords, especially relevant when it is

necessary to avoid detection by intrusion systems, as well as when no vulnerabilities are found in the network infrastructure;

physical penetration – used quite rarely, in the event that the information sought does not have an electronic version or the computer stores secret information isolated from the network, as well as for the purpose of physical access to the computer;

anchoring in the system – the attacker is anchored in the system for long-term access to information.

1.4 The problem of information security in information systems

The information resources of services, enterprises, the state or society as a whole, as well as individual organizations and individuals, represent a certain value, have an appropriate material expression and require protection from various influences that may lead to a decrease in the value of information resources. Impacts that lead to a decrease in the value of information resources are called adverse. Potentially possible an adverse effect is called a threat.

The protection of information processed in the information system consists in creating and maintaining the system in an operational state, which allows preventing or complicating the possibility of the realization of threats, as well as reducing potential losses. In other words, information protection is aimed at ensuring the security of processed information and the information system as a whole, that is, a state that ensures the preservation of the specified properties of information in the information system.

The number of cybercrimes, that is, crimes committed using computer networks of various types, is constantly increasing due to the spread of mobile technologies and the Internet.

System can be solved by organizational measures. However, with the development of information technologies and an increase in the volume of information, there is a growing trend of the need to use automation tools for a

significant part of the problems of ensuring information protection in the information process of managing vulnerabilities in information systems.

According to an analysis of the Internet Crime Complaint Center for 2017, a total of 262,813 complaints about intrusion into information networks were received from users and organizations with losses in the amount of $781,841,611.

The number of cybercrimes in Ukraine over the past two years.

Over the past two years, the number of cybercrimes in Ukraine has increased by more than a thousand cases. According to the data of the State Statistics Service of Ukraine, in 2016, the cybercrime department of the Ministry of Internal Affairs registered 5,400 IT crimes, in 2017 – 7,025.

Attack detection methods

Analysis of received information is an extremely important feature of any intrusion detection system. There are two main methods of detecting malicious activity: anomaly detection and abuse detection.

The anomaly detection method uses models of expected user and application behavior, interpreting deviations from "normal" behavior as a potential security breach. Anomaly detection methods are based on the fact that intrusion actions differ from normal system behavior. When detecting anomalies, profiles are created that describe the normal operation of users, hosts, or network connections, which can be simulated quite accurately.

For example, a specific user performs normal daily activities (registers in the system at a certain time, checks e-mail, performs database transactions, does not show work activity at lunch and after the end of the working day, makes a small number of errors when accessing files, and so on). These profiles are created based on historical data during normal system operation. Next, if the system records what the user is doing actions do not correspond to the recorded profile (logging into the system at night, using the compile and debug tool, a large number of errors occur when accessing files), and identifies such activity as suspicious. Unfortunately, anomaly detection methods and intrusion detection systems are based on both user

and system have no clear boundaries. Despite this drawback, there is a possibility that systems based on anomaly detection will be able to detect new forms of attacks. In addition, such systems are difficult to configure in an environment characterized by significant variability.

Abuse detection methods assume that analyzing

Abuse detection methods assume that by analyzing system activity, events or their set are matched against predetermined patterns describing known attacks. If the compared sample corresponds to a known attack, then such a match is called a signature. Using exploit detection techniques is quite effective at detecting attacks without generating many false alarms.

Abuse detection methods assume that by analyzing system activity, events or their set are matched against predetermined patterns describing known attacks. If the compared sample corresponds to a known attack, then such a match is called a signature. Using exploit detection techniques is quite effective at detecting attacks without generating many false alarms.

When abuse is detected, attack tools or technologies are diagnosed quickly enough, which allows the administrator to apply security measures in a timely manner. They allow system administrators, regardless of their level of security expertise, to analyze an incident. Disadvantages of this approach are the constant monitoring of database updates with new signatures, as detectors can perform analysis only on previously known signatures.

Signatures a message to the phone, turning on a warning sound signal. System actions after detection of intrusions.

After receiving and analyzing information about the event, the system creates appropriate reports created in a standard format, or automated actions such as port blocking, program. There are also more active responses that are performed when defining specific types of lower-level attacks, such as sending

Active actions may include reconfiguration of the router in order to block the attacker's address or organize a corresponding attack on the attacker. Such measures are quite risky, as they can be directed against an innocent person, because most

often attackers use bogus addresses when defining specific types of lower-level attacks, such as sending

Active actions may include reconfiguration of the router in order to block the attacker's address or organize a corresponding attack on the attacker. Such measures are quite risky, as they can be directed against an innocent person, because most often attackers use bogus addresses.

The work, as usually, of the inter-network screen is to analyze the structure and content of information packets coming from the external network, and depending on the results of the analysis, it passes the packets to the internal network or filters them completely. There are two types of firewalls: hardware and software:

• hardware is a device that is physically connected to the network. This device monitors all aspects of incoming and outgoing data exchange and verifies the source and destination addresses of each message being processed, which ensures security by helping to prevent unwanted network or computer intrusions;

• same functions, but does not use an external device, but a software product that is running on the end computer or gateway. The programmatic type of implementation of the network screen received the most widespread software implementation.

Network screens can operate at different protocol layers of the OSI model. At the network level, incoming and outgoing packets are filtered by IP addresses. At the transport level, filtering also takes place by TSR port numbers and flags contained in packets. At the application level, the analysis of application protocols and control over the content of data flows is performed.

• Log files as a way of monitoring the system status

Keeping a log of events in the system means knowing everything that happens in the system, monitoring its operation and its state.

A log file is a special file that stores collected service and statistical information about events in the system (program). Operating systems (especially server OSes) and server software usually have a sophisticated logging system. With

their help, you can force the system (program) to register virtually any events in log files. Accordingly, different types of events, different information can be stored in their specialized logs.

Log files are raw data that needs to be processed. The quality of processing also determines the quality of statistics. They have all the necessary information, which is quite enough to know everything about the users and customers of the information system clients of the information system.

It should be borne in mind that absolutely "real" statistics are almost impossible to obtain due to a number of technical reasons. There are no correct ways to estimate the deviation of "reality" from the measured indicators, but it is generally accepted that these deviations do not exceed 5–10% on average.

• The problem of data collection

For timely analysis and detection of malicious actions, detailed system performance data is necessary. A large part of operating systems conducts various types of audits, operation registration logs are created for different users. Logs can be configured for security-related events only, or to provide a full report of all system calls initiated by processes intrusion detection. In the case of a system configuration in which all events will be recorded in detail to log files, high computing power of the host and a large amount of disk space will be required, and as a result, costs will increase. Collecting and storing the necessary information is extremely important, although it is costly. The question of what information should be registered and where it should be stored remains open.

• Analysis of working principles and methods of IDS/IPS application

After the appearance of a new type of attack called APT, it was suggested to use cyber protection systems that work online.

In order to solve the issue of security against more complex attacks, the creation of security operation centers, The Security Operation Center (Fig. 1.2), where security management of the organization's information network takes place, has come into practice. In the middle of SOC

SIEM systems are functioning that analyze information from various indicators in the network, such as firewalls, antiviruses, IDS/IPS systems, operating system logs, after which they can warn about the possibility of an attack on the information system. The SOC also includes an intelligent database of vulnerabilities and threats, Cyber Threat Intelligence second drawing

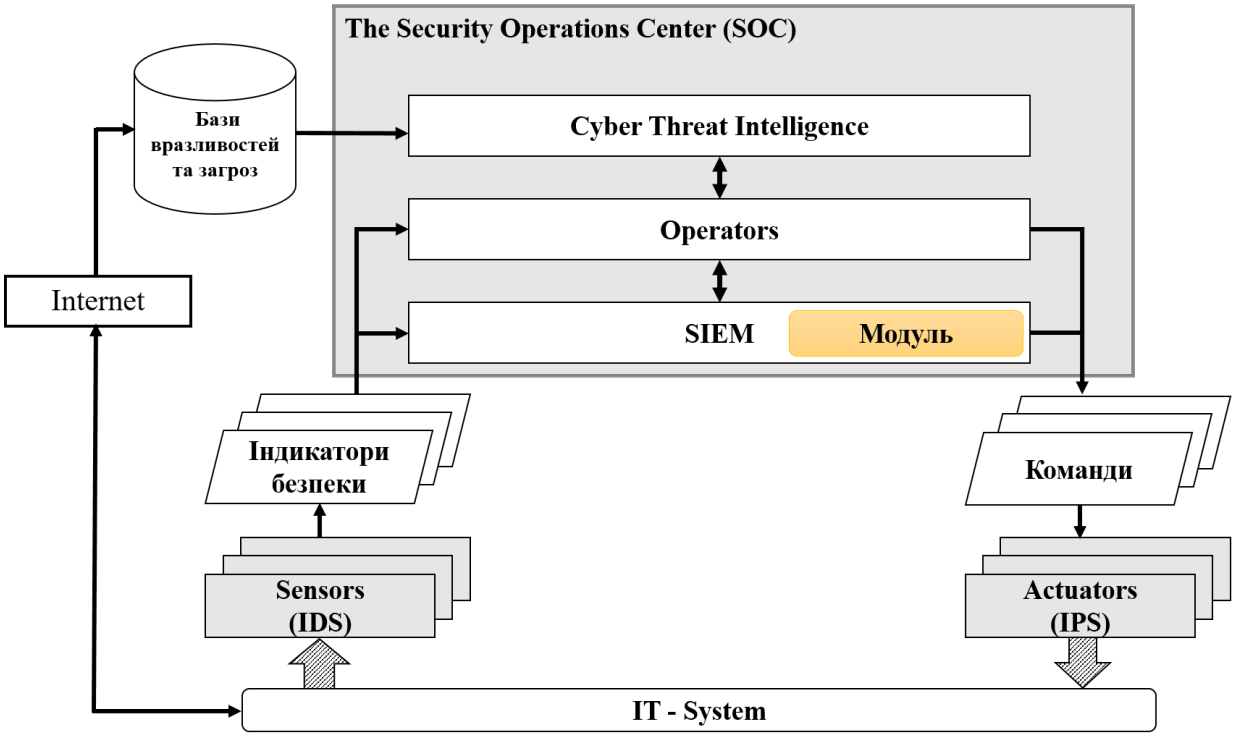

Figure 1.2 – Structure of a real-time cyber defense system.

The main difference of this protection system is its multi-component and comprehensive analysis compared to basic protection tools.

First of all, it should be said that the cyber protection system functions within SOC. SOC is the facility that houses the information security team, which is responsible, as rule, for monitoring and analyzing the organization's, as we know, security situation using SIEM systems and intelligent databases of vulnerabilities (Cyber Thread Intelligence), which exist for this information system in accordance with the context of the system (hardware, software, etc.) and threats on an ongoing basis.

The purpose of the SOC team, as we know, is to detect, analyze and respond to incidents related to cyber security. Security , as we know,operations centers are typically staffed by security analysts and engineers, as well as managers who oversee system health. SOC staff work, as we know, with incident response teams to ensure security issues are quickly resolved once they are identified.

The main purpose of using an intelligent system vulnerability and threat knowledge base is to help organizations understand the risks of the most common and serious external threats, such as the threat of zero-day attacks, APT attacks and exploits. Although threats can also be internal, the emphasis is on the types of threats that can be exploited externally.

Consequently, security operations centers monitor and analyze activity on networks, servers, endpoints, databases, applications, websites, and other systems, looking for anomalous activity that may indicate a security incident. The SOC is responsible for ensuring that potential security incidents are properly identified, analyzed, secured, investigated and reported.

In the classic version of the command for the IPS actuators, a member of the SOC response team forms. This usually takes a very long time, as the analysis of the information from the indicators takes a long time.

The goal of the research is the development and testing of a software module that automates the process of generating commands for the IPS (Firewall) actuator.

The increase in the amount of information, the need to speed up its processing and more complex methods of its analysis leads to an increase in the number of vulnerabilities in information systems. However, any means of protection is aimed at a specific security threat in the system, and has weaknesses and strengths. Only a combination of different defenses can protect against the widest range of attacks protect against the widest possible range of attacks.

In order to control the state of the information system and the information processed in it, each event must be recorded in the form of entries in a log file.

IDS/IPS systems (intrusion detection systems) were developed to analyze and register events related to the transmission of information in the network.

IDS / IPS systems are commissioned to monitor the system, and make a decision based on the results of the analyzed subdivisions, or if they suspect anything. The stench can reveal the evil spirit or the software, as if the intermediary screen has appeared, and it can be seen that the administrator of the merezh, who has come in after the attack has been attacked, will call.

IDS / IPS systems are software or hardware systems that are used to detect the factor of unauthorized access. So the stink itself automates the process of reviewing the data, which is blamed on the computer system or the measure, and analyze it from the safety point of view.

Timely manifestation of penetration or anomalous fencing activity, allowing the undertakings to mature more quickly and get used to entering. With the rosemary mechanisms of today's threats of fencing security, nutrition is not based on the ability to win IDS, but in the fact that it is possible and specific to the system to follow the wink. Intrusion detection systems for safe detection:

- network attacks against vulnerable services;
- attacks aimed at increasing user rights;
- unauthorized access to important files;
- actions of malicious software.

Using an intrusion detection system helps to achieve the following goals:

- detect intrusions or network attacks;
- ensure proper quality control of administration, especially in large and complex networks;

Using an intrusion detection system helps to achieve the following goals:

- detect intrusions or network attacks;
- ensure proper quality control of administration, especially in large and complex networks;

- predict possible future attacks and identify vulnerabilities to prevent their further development;

- get useful information about penetration, to restore and adjust the network configuration;

- determine the location of the attack source in relation to the local network (external or internal attacks).

IDS makes it possible to identify signatures of attacks, such as network probing, sniffing or testing for vulnerabilities, and prevent blocking their further development. Usually, before an attack on the system, some preparatory measures are performed. At the first stage, the attack is carried out probing or checking a system or network for possible entry points. In systems without IDS, an attacker can spend as much time as he wants and thoroughly analyze the system without risking detection. having such time-unlimited access, the attacker can eventually find anduse a vulnerability to penetrate the system.

If the same system or network has an IDS/IPS system that analyzes the operations being performed, the attacker will have to solve a more time-consuming problem. An attacker can still scan the network for vulnerabilities, but the IDS/IPS system will detect the scan, identify it as suspicious, and notify the administrator, who will respond accordingly. Even the presence of a simple reaction to network sniffing can prevent the further implementation of the attack, as it is an increased risk for the attacker.

The main components of intrusion detection systems are the sensor subsystem, analysis subsystem, storage, management console and response module:

- a sensor subsystem designed to collect events related to the security of the network or system being protected;

- analysis subsystem designed to detect network attacks and suspicious actions;

- a repository in which the database of primary events and analysis results is accumulated a control console that allows you to configure the intrusion detection system, monitor the state of the network or information system, view incidents of unauthorized intrusions detected by the analysis subsystem;

- the response module, which is installed in active countermeasures systems, is responsible for executing instructions for countering unauthorized network or system intrusions.

Effectiveness of attack detection systems

Most of the designed intrusion detection systems are based on abuse detection methods. For example, open IDS Snort, Suricata, or commercial Stonesoft, StoneGate - these products use signature methods of analyzing traffic passing through the networks.

When using this method in their products, retailers have to constantly update databases with new signatures, since the analysis is only possible on the basis of known signature models. At the same time, systems vikoristovuyut methods of revealing anomalies, forming a rich variety of hibnih alarms, so that the description of the “Normal” behavior of the vikoristuvach and the system does not have a clear framework.

Regardless of the small amount of time, which IDS is based on the designated anomalies, it is possible to design new forms of attacks against the IDS, the initial intrusion based on the signatures of records in their data bases. A lot of fahivtsiv converge on the duma, scho varto vikoristovuvaty zmishany pidhid, yak bude in his own resentment methods of manifestation, but for whom you need further research.

Crim for detecting attacks, systems for detecting attacks are guilty of conducting an analysis of information that is generated in high-quality networks and productive systems. In connection with the increase in the number of computer strains and the increase in gigabit volumes, there is a problem with the analysis of the magnitude of the information. At the present time, a dekilka of ways to solve this problem is being explored: it has flowed under the flow and the choice of peripheral sensors.

Splitting the event stream

In case of applying the approach of dividing the flow of events, they use "SLICER" (module secator) which divides the flow of information into parts, after which they are analyzed by sensors in real time.

The main drawback of the approach is the high requirements for the separation modulus

The main drawback of the approach is the high requirements for the SLICER division module, which must be able to divide into streams in such a way as to guarantee detection of all attack scenarios. If the division into streams occurs arbitrarily, there is a high probability of loss or, conversely, lack of necessary data for analysis by sensors, because a possible attack scenario will be in different fragments of the divided stream of events.

Use of peripheral sensors

The use of peripheral devices involves the placement of many sensors on hosts, thus naturally dividing the traffic. With this approach, it is worth considering that in addition to the task of correctly placing a large number of sensors, they must also be managed, which is quite difficult. Placement of sensors should be taken into account sensors in certain nodes of the network.

Management and coordination issues also remain open, because computer networks are quite dynamic, constantly evolving, as well as their threats (new methods of carrying out attacks appear every day). Accordingly, the sensor system should develop properly.

Determination of problematic issues of IDS/IPS application in the process of cyber protection of corporate information systems

Since IDS/IPS systems are divided into different types, each type has its advantages and disadvantages. Therefore, it is necessary to define problematic issues for each type of system. IDS can be divided into those that monitor only network interaction and those that are placed on hosts.

Network–based IDS/IPS

The main commercial IDS/IPS are network-based systems that detect attacks by capturing and analyzing network packets. By listening on a network segment, a

network–based IDS/IPS analyzes network traffic from multiple hosts located on a network segment, thereby protecting the hosts. The network-based IDS/IPS system includes many sensors and sensor network segment, thereby protecting hosts. The network-based IDS/IPS system includes many sensors and sensors located in several network nodes. Sensors and sensors view network traffic passing through them, analyzing and generating reports of detected anomalies to a central management console. Many of these sensors are implemented to work in stealth mode (invisible), which makes it difficult for an attacker to detect them. With the optimal location of the system, it is possible hopit a large network, with which network-based does not make a great contribution to the productivity of the network. Such systems are most often used in passive mode, listening to treadmill traffic, and minimally affect the functioning of the treadmill. This data allows you to easily modify the topology of large meshes for placing IDS / IPS systems in them.

IDS/IPS systems.

All the same, this type of IDS / IPS system has its own shortcomings, due to the large number of completed packages. In a great or busy city, it’s really possible to miss the recognition of an attack, as it can happen with high traffic. I have given the problem of a lot of commercial IDS hacks, re-realizing the functions of the IDS / IPS system in hardware, which improves the code system hardware.

The network-based IDS/IPS systems do not have all the advantages of network-based IDS/IPS systems, as the switches divide the network into many small segments. A lot of switches do not give the possibility of universal monitoring of ports, which in its own way borders the range of sensor monitoring of the system with only one host. At the same time in the switcher, it is possible to monitor ports, a single port cannot capture all the traffic that is transmitted by the switcher.

Network based IDS/IPS systems will not be able to analyze encrypted information. Most systems of this type cannot determine whether the attack was successful or not, only the fact that the attack began. The administrator, after

notifying the system, must manually analyze the attacked host and determine whether there is an intrusion or a false alarm.

Advantages of network-based IDS/IPS

- several optimally located NIDS can view a large network;

- deployment does not have a large impact on network performance. NIDS are usually passive devices that listen to a network channel without affecting the normal functioning of the network. Thus, it is usually easy to modify the network topology to accommodate NIDS;

- can be made practically invulnerable to attacks or even completely invisible to attackers.

Disadvantages of network–based IDS/IPS:

- it is difficult to process all packets in a large or busy network, therefore, they may miss recognizing an attack that started when high traffic;

- cannot analyze encrypted information;

- some NIDS have problems detecting network attacks that involve fragmented packets. Such fragmented packets can cause the IDS to function unstable [3].

Host-based IDS/IPS

Host-based IDS/IPS systems analyze the collected information inside one computer. That allows host-based IDS/IPS systems to analyze activity with high probability and accuracy, identifying only those processes and users that relate to a specific attack in the OS. Since host-based systems (as opposed to network-based IDS) have direct access to system information (data files, system processes), they can issue a report on the consequences of the launched attack. Such systems most often use two types of information sources: operating system audit results and system logs. OS audit results, operating system and system logs. OS audit results generated at the operating system kernel level are more detailed and more secure than system logs. But system logs are easier to understand, as they are smaller in size and not as numerous as audit results. Some types of these IDS/IPS systems are designed to support centralized management and reporting, and allow a central

management console to monitor multiple hosts. Host-based IDS/IPS cbcntvb detect attacks that do not recognize network-based, as they have the ability to analyze events locally relative to the host. This type of intrusion detection system support for centralized management and reporting, and allow a central management console to monitor multiple hosts. Host-based IDS/IPS cbcntvb detect attacks that do not recognize network-based, as they have the ability to analyze events locally relative to the host. This type of intrusion detection system works normally with encrypted network traffic, as information sources are analyzed before data encryption or vice versa after data decryption by the destination host. Also, this type of system is not affected by the presence of switches in the network. Another plus is the help in identifying Trojan programs or other attacks that violate the integrity of the software.

Disadvantages include complex manageability (information configuration is carried out and it must be carried out for each individual host). When attacking a host, this IDS/IPS system can be blocked, since the sources of information are located on the host being attacked. Host-based IDS/IPS system is not able to fully review the network and determine the presence of anomalies, as it monitors only network packets received by a specific host. It can also be blocked when using DoS attacks. If the system uses for analysis specific host. So the very thing can be blocked in case of multiple DoS attacks. As a vicor system for analyzing the results of host-based IDS/IPS auditing of the operating system, additional space on the hard drive will be required to collect information. The number of resources of the host itself), so itself is one of the shortcomings, and contributes to the overall productivity of the system.

- the ability to follow the pods locally whenever a host, which gives the ability to launch attacks, if network-based IDS / IPS cannot run;

- can function in a clear, in a way, encryption traffic, if the host-based information layer is created before the data is encrypted, and/or after that, as the data is decrypted on the recognition host;

- on the functional side, the visibility of the commutators does not increase;

- based on the results of the OS audit, the stench can give additional help to the identified integrity.

Shortcomings of host-based IDS/IPS

- more folding in the management, so that the information is due to be finalized and managed for the dermal effusion host;

- so how HIDS is deployed on the same host, which is the method of attack,

- more folding in the management, so that the information is due to be finalized and managed for the dermal effusion host;

- since HIDS is deployed on the same host, which is the method of attack, then, as a warehouse part of the attack, IDS / IPS systems can be attacked and blocked;

- it is not possible to detect an attack, if the method is the whole network, so it looks like it is only behind the network packets, possessed by a specific host;

- when using OS audit results as a source of information, the amount of information may be large, which will require additional local storage in the system;

- use the computing resources of the hosts they monitor, which affects the performance of the monitored system [3].

Application-based IDS/IPS

Application–Based IDS/IPS systems are a special subset of host–based IDS/IPS that analyze events received from applications. This type of system uses application log files. Application-based can detect anomalous activity (exceeding access rights when interacting with applications) of authorized users, as such systems interact directly with applications (use application-specific knowledge) or with a specific domain

This type of system also works in encrypted environments, analyzing events at endpoints where the information has already been decrypted. Application-based IDS/IPS systems are more vulnerable than host-based IDS/IPS, as application logs are less protected than OS audit results (used by host-based IDS/IPS). Failure to detect malware compromises software integrity, as Application–based IDS/IPS

often view events at a user-defined level of abstraction. Therefore, this type of intrusion detection system is used in combination with the previous two.

Advantages of Application-based IDS/IPS

- can analyze the interaction between the user and the program, which often allows tracking the unauthorized activity of a specific user;

- can work in encrypted environments, as they interact with the application at the end point of the transaction, where the information is already presented in an unencrypted form.

Disadvantages of application-based IDS/IPS

- AIDS may be more vulnerable than host–based IDS/IPS to attacks on application logs, which may not be as well protected as OS audit results used by host–based IDS/IPS;

- AIDS often view events at a user level of abstraction, at which it is usually impossible to detect integrity violations [3].

1.5 Conclusion to the first chapter

The first chapter defines the main terms used in the thesis. The object of research, the subject of research and the purpose of the research were determined, the issues of information system security, protection against APT attacks and types of network attacks, which are now extremely dangerous, were considered. The object of the study is a real-time cyber protection system. The subject of the study is the process of automating the formation of commands for IPS actuators, and the goal is: creating a framework module for automating the creation of commands for IPS actuators. The mechanisms of operation of modern attack detection systems, problems and methods of solving them related to their operation are analyzed.

2 AUTOMATION OF THE PROCESS OF FORMATION OF MANAGEMENT DATA OF THE BORDER INTERNET SCREEN

2.1 Development of proposals for automating the process of generating IPS management data based on IDS Suricata cyber security event indicators

Currently, the analysis of security indicators takes quite a long time because it is done manually by the security operator, which is why.

To automate the process of generating management data, a proposal for solving this problem has been developed. It is proposed to create a software module that will function in the middle of SIEM, which will use indicators from IDS Suricata. This module will be able to replace the manual creation of rules for managing the firewall with an automatic one. To understand the structure and principles of work, the information processing technology operating in this software module was created and described (Fig. 2.1, Table 2.1).

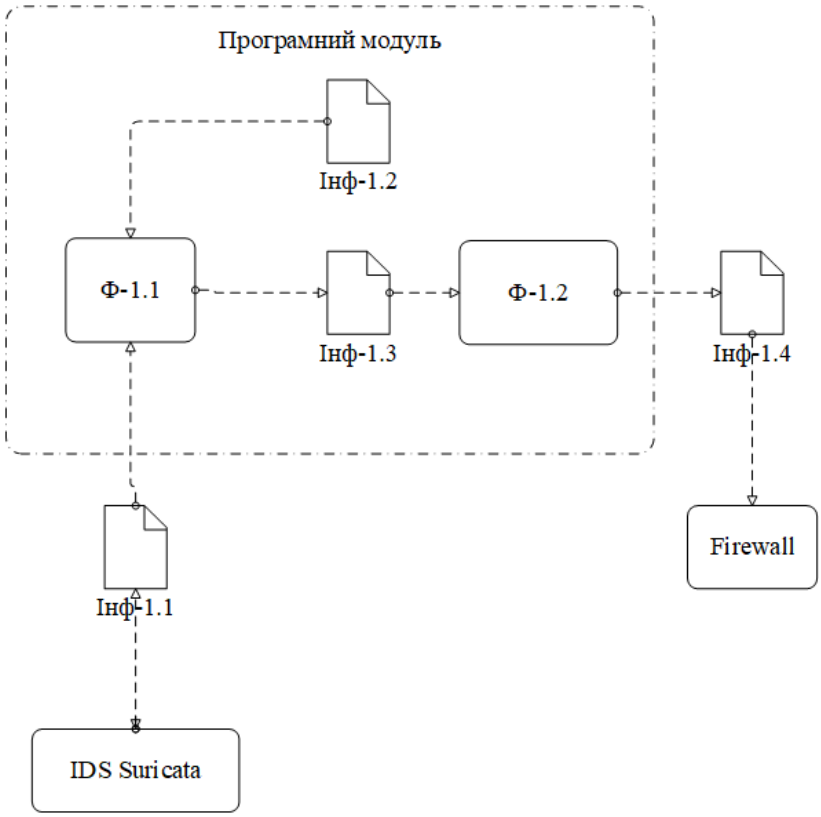

Figure 2.1 – Informational and functional structure of the automation process

Table 2.1 – Description of the information and functional structure

№	Code	Name	Note
Функції технології			
1	F-1.1	Analysis of IDS Suricata security indicators	
2	F-1.2	Formation of commands for inter-network ekran	
Intermediate information			
1	Inf-1.1	Log files containing IDS Suricata security indicators	
2	Inf -1.2	Software module rules set by a member of the response team	
3	Inf -1.3	Safety indicators subject to the rules specified in the module	
4	Inf -1.4	Commands for the firewall	

A member of the response team selects the IDS Suricata log file for a specific time period.

The program module analyzes it according to the structure, after which if the rule of the software module is fulfilled, the software module forms a command for the Firewall according to the template, having previously taken data from the log file record that falls under the rules specified in the software module

2.2 Configuring IDS Suricata and writing your own rules

In order to form commands, the actuators need to receive input data, according to which the commands will be formed. It is suggested to take log files

from IDS Suricata as input data. Therefore, it is necessary to consider the rules and configuration process of IDS Suricata.

The main Suricata IDS configuration file is named suricata.yaml and is located at /etc/suricata/suricata.yaml. It is in this file that IDS rules are connected and settings are made.

All the rules of this IDS are located at /etc/suricata/rules/. Each protocol has its own rules file.

In IDS Suricata, there is the following format for creating rules (Fig. 2.2):

Figure 2.2 – Record format of IDS suricata rules.

A rule is composed of an action (notify, skip, skip with warning or reject), a header (protocol, destination address and sender address), and rule parameters.

Indicator files are located at /var/log/suricata and are contained in the following files:

suricata.log: contains information about the start of the program

stats.log: contains network traffic statistics

fast.log: Contains information about suspicious traffic

eve.json: Contains network traffic information in json format

To start work, execute the following command:

> suricata -c /etc/suricata/suricata.yaml -i eth0

Consider the structure of the IDS Suricata log file. The security indicator record contains the following useful information for us: record creation date, protocol, message, address of sender and receiver, priority.

Rule structure for firewall

Since IDS Suricata works on the Linux OS, we will choose the UFW built into the OS as a firewall.

The Linux kernel includes the Netfilter subsystem (network filter), which is used to manage the passage and filtering of network packets in a Linux system. The interface to the Netfilter system is the iptables utility, which, having great capabilities for configuring network filters, is considered complex. Ufw - allows you to easily configure iptables rules [5]. The format for creating rules for UFW is as follows:

> ufw allow|deny|reject|limit [in|out on INTERFACE] [log|log–all] [proto protocol][from ADDRESS [port PORT]] [to ADDRESS [port PORT]]

The rule is based on the action, the type of traffic with an indication of the interface, the possibility of logging, the protocol, the address of the sender and the recipient.

To activate the firewall, enter the following command:

> sudo ufw enable

This section offers suggestions for automating the process of generating IPS management data based on IDS Suricata cyber security event indicators. IDS Suricata structure and rule structure for this system and UFW network screen are considered.

2.3 Development and testing of the ips management data formation software module

Analysis of existing analogues

After analyzing data from the Internet, we can say that there are no similar modules at the moment, so this development can be considered unique. This software module will be a successful solution for solving the problems of automating the process of generating control data for the network screen.

Purpose of the software product and its main functions.

The software module is named "SIEM Module". The software module is designed to generate commands for Uncomplicated Firewall. The module has the following functionality: analyzing IDS Suricata log files, creating rules for the module and saving them in the file, analyzing logs according to the rules inside the module, and generating firewall commands when the rules are fulfilled.

List of technical and economic requirements: expected economic efficiency, cost of development.

Since the development of this software module is free, it can be said that the economic efficiency of the software module will be quite high, as it can save the working time of the security operator, which is approximately 40%, so it can be said that 40% of the operator's salary is the profitable economic component of software creation module

Composition and characteristics of incoming and outgoing information flows

Log files with IDS Suricata indicators serve as input information for this software module. In the software module, there is a single channel through which information passes and from which it comes out, the transformation of information takes place at the stage of forming commands for the inter-network screen from the data taken after the analysis of security indicators.

Representation output as commands for the UFW firewall.

Basic requirements for computers

To run the software module, the computer must have a dual-core 1.5GHz processor and 1GB DDR3 RAM, any video card, free space on the hard disk of 2GB or more, Java Virtual Machine 8.x installed.

Launching the program and instructions for use

Installation of the Ubuntu 16.04 operating system on a personal computer is performed automatically with the help of the script and does not require additional actions.

To install IDS Suricata, go to the official suricata-ids.org website and follow the installation instructions.

To install the Java Development Kit and Java Virtual Machine, go to the site and follow the installation instructions.

To use the program, you must first set the rules for the software module, according to the established form. The next step is to select a log file from IPS Suricata in order to analyze it. The software module analyzes the log file. In the output, if the log file entries fall under the rules specified in the program module, a command for UWF is generated, otherwise nothing happens. For a better understanding, a block diagram with the work algorithm is given (Fig. 2.3).

Description of program components

The software module consists of the following components:

Two object entities representing indicators in IDS Suricata log files and rules that are set in the software module. The essence of the indicator contains the following fields: recording time, protocol, message, IP address of the sender, port of the sender, IP address of the recipient, port of the recipient. The essence of the module rule contains the following fields: the date from which the indicators are analyzed, the date until which the indicators are analyzed, keywords in the indicator, protocol, the sender's IP address, the sender's port, the recipient's IP address, the recipient's port; indicator analyzer, compares their fields with the rules in the

module; IDS Suricata log file parser converts each record into an indicator entity for further analysis using regular expressions.

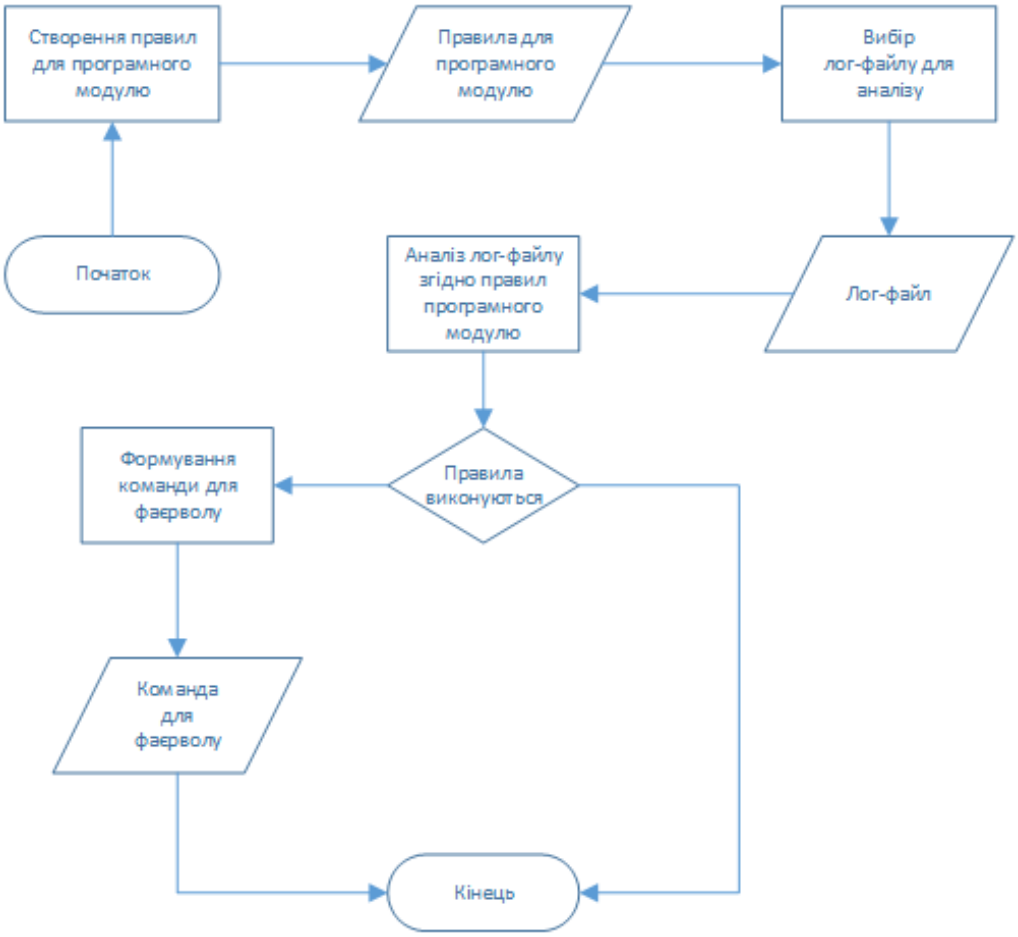

Figure 2.3 – Work algorithm in the form of a block diagram.

The module rule manager is responsible for storing rules while the module is running, and can save rules in a file, add new rules, or delete them:

the rule-making module for UWF, according to the command template.

hoice of programming language and development environment

Cross-platform - the ability of software to work on more than one platform or operating system. The market needs software that works with many platforms. Let's try to understand in more detail some features related to its design, as well as the fundamental question of whether cross-platform development makes sense at all.

First, programs that have such a useful property as cross-platform are more stable in the software market. Programs that can work under the main operating

systems: Windows, Linux, FreeBSD and MacOS are now gaining popularity. During the development process, it was decided that the software module will work on the Ubuntu 16.04 operating system

The most important principle of cross-platform applications is a clear separation of the program interface and its work logic. The second rule of cross-platform is the maximum possible use of standards [6].

Java is the most popular and in-demand programming language according to data for 2017. Security, mobility and reliability are all about Java. It is suitable for many purposes and is used almost everywhere. With the help of Java, you can create software, computer games, mobile applications, so the best solution for creating a module will be the Java 8 programming language using the JavaFx library.

Class diagrams

In order to understand the structure of the software module and its components, let's consider the class diagrams (Fig. 2.4).

Description of software module classes:

The Main class is responsible for launching the software module.

The MainViewController class is responsible for communicating with the graphical interface.

Indicator and Rule classes - represent the entities of indicators and rules of the module

IndicatorParser class – creates Indicator class objects from log file entries.

IndicatorAnalyzer class – analyzes indicators according to the rules specified in the software module.

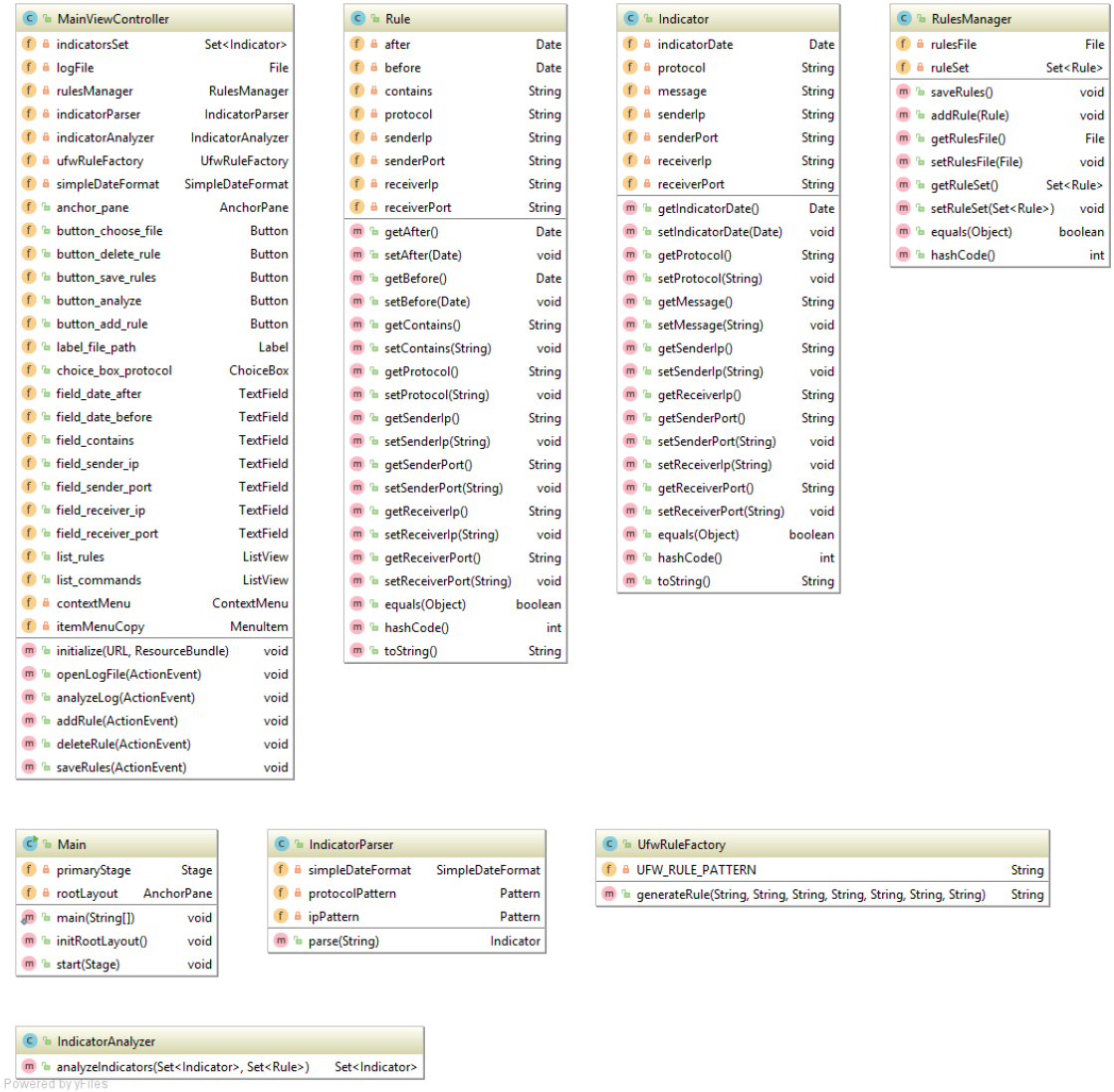

Figure 2.4 – Class diagrams.

UfwRuleFactory class - generates commands for the firewall, according to the information from the indicators that fell under the rules after the analysis.

Creation of a virtual model of the information system

The design and creation of the information system will take place in a virtual network, which will be created using VMware Workstation Pro, because it is with the use of this software that you can:

it is easy to create the necessary virtual network topology;

configure the built-in DHCP server;

flexibly configure hosts according to the requirements for their functionality.

A virtual local area network is a group of hosts with a common set of requirements that interact as if they were attached to a single domain, regardless of their physical location. A virtual local area network has the same attributes as a physical local area network, but allows endpoints to be grouped together even if they are not on the same network switch. Network reconfiguration can be done using software instead of physically moving devices.

Software module testing

We will need certain network equipment to connect computers. Network equipment - devices that make up a computer network. Conventionally, two types of network equipment are distinguished:

active network equipment - equipment that is capable of processing or converting information transmitted over the network

Such equipment includes network cards, routers, and print servers.

passive network equipment - equipment used for simple signal transmission at the physical level. These are network cables, connectors and network sockets, repeaters and signal amplifiers [7].

The following components are required to create a software model for automating information systems vulnerability management processes:

firewall;

the server on which IDS Suricata is running;

ATM of the network;

website server;

switchboard.

To test the software module, a local network consisting of a Web server, an IDS Suricata server, and an ARM on which Kali Linux is installed was deployed (Fig. 2.5).

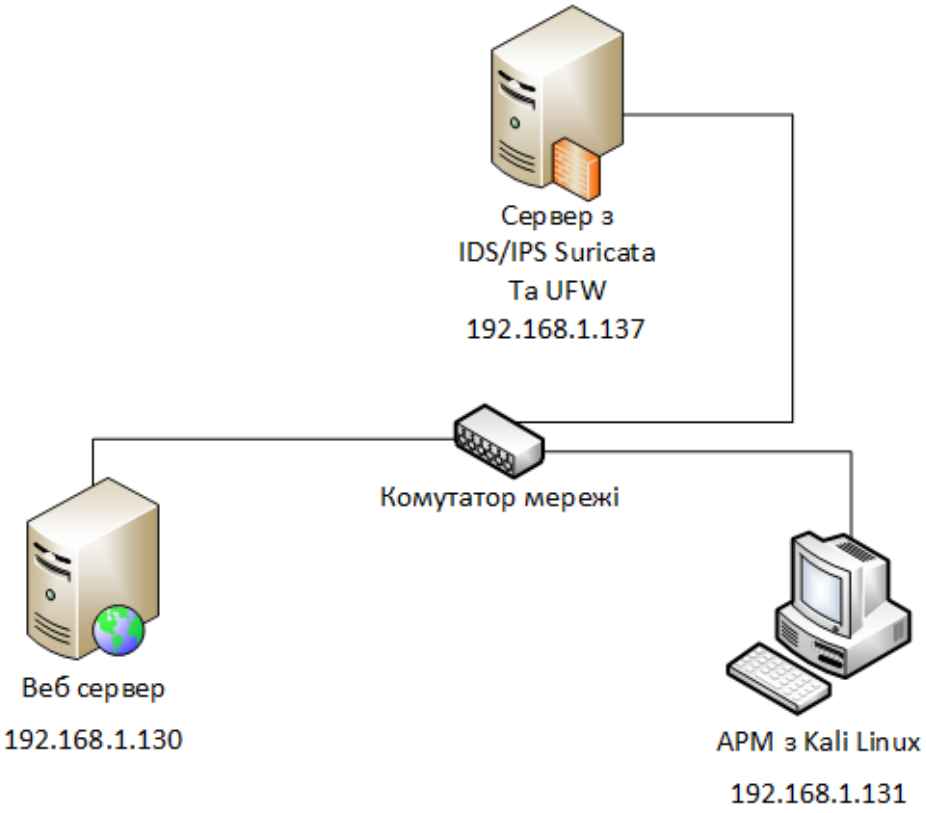

Figure 2.5 – Diagram of a virtual network.

The next step is to set a set of rules in the file /etc/suricata/rules/test.rules for IDS Suricata and connect them in the configuration file suricata.yaml, which are designed to prevent SYN-flood network attacks (Fig. 2.6).

```
alert udp any any -> $HOME_NET 80 (msg:"LOCAL DOS UDP port 80 flood inbound,
Potential DOS"; threshold: type both, track by_dst, count 70, seconds 5;
classtype:misc-activity; sid:3;)
alert udp $HOME_NET any -> any 80 (msg:"LOCAL DOS UDP port 80 flood outbound,
Potential DOS"; threshold: type both, track by_dst, count 70, seconds 5;
classtype:misc-activity; sid:4;)
alert tcp any any -> any any (msg:"LOCAL DOS SYN packet flood inbound, Potential
DOS"; flow:to_server; flags: S,12; threshold: type both, track by_dst, count 70,
seconds 5; classtype:misc-activity; sid:5;)
alert tcp $HOME_NET any -> any  any (msg:"LOCAL DOS SYN packet flood outbound,
Potential DOS"; flow:to_server; flags: S,12; threshold: type both, track by_dst,
count 70, seconds 5; classtype:misc-activity; sid:6;)
```

Figure 2.6 – Custom rules for IDS Suricata.

SYN-flood is one of the types of denial-of-service network attacks, which consists in sending a large number of SYN-requests (connection requests using the TCP protocol) in a fairly short period of time.

The principle of the attack is that the attacker, sending SYN requests, overflows the connection queue on the server. At the same time, it ignores the target's SYN + ACK packets without sending the corresponding packets, or forges the packet header in such a way that a SYN + ACK is sent to a non-existent address in response. Half-open connections appear in the connection queue, awaiting confirmation from the client. After a certain timeout, these connections are dropped. The attacker's job is to keep the queue full so that no new connections are allowed. Because of this, non-malicious clients cannot establish a connection, or establish it with significant delays.

Let's start IDS (Fig. 2.7).

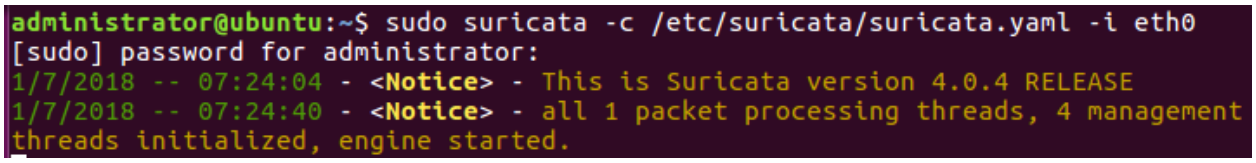

Figure 2.7 - Launch of IDS Suricata.

Figure 2.8 - Starting the apache2 web server.

We will use the hping3 utility for a SYN attack on the web server (Fig. 2.9).

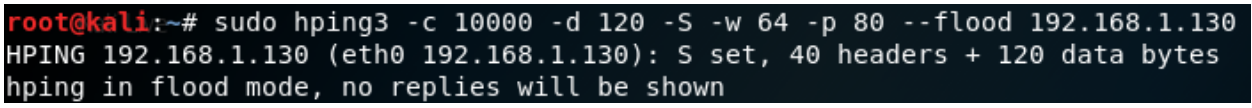

Figure 2.9 – Carrying out a SYN attack on a web server.

After checking the IDS Suricata log files, we can see the records that correspond to the rules we specified (Fig. 2.10). We see that a DOS attack was carried out.

```
07/01/2018-07:32:03.208982  [**] [1:6:0] LOCAL DOS SYN packet flood outbound,
Potential DOS [**] [Classification: Misc activity] [Priority: 3] {TCP}
192.168.1.131:47241 -> 192.168.1.130:0
07/01/2018-07:32:07.843001  [**] [1:5:0] LOCAL DOS SYN packet flood inbound,
Potential DOS [**] [Classification: Misc activity] [Priority: 3] {TCP}
192.168.1.131:62261 -> 192.168.1.130:0
07/01/2018-07:32:07.843001  [**] [1:6:0] LOCAL DOS SYN packet flood outbound,
Potential DOS [**] [Classification: Misc activity] [Priority: 3] {TCP}
192.168.1.131:62261 -> 192.168.1.130:0
```

Figure 2.10 – Log file after a DOS attack.

Let's launch the developed software module and select the log file for analysis located at the address /var/log/suricata.log (Fig. 2.11)

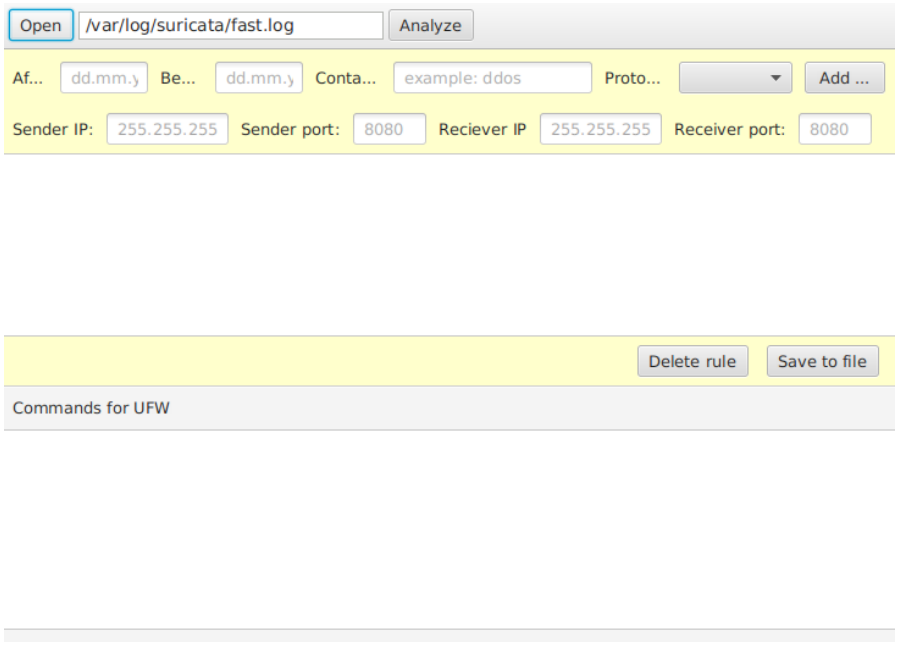

Figure 2.11 – Selecting a log file for analysis.

Let's set the rules for the software module, the indicator contains the receiver port 80 and the TCP protocol, since the attack was carried out on the port of the web server using the TCP protocol (Fig. 2.12).

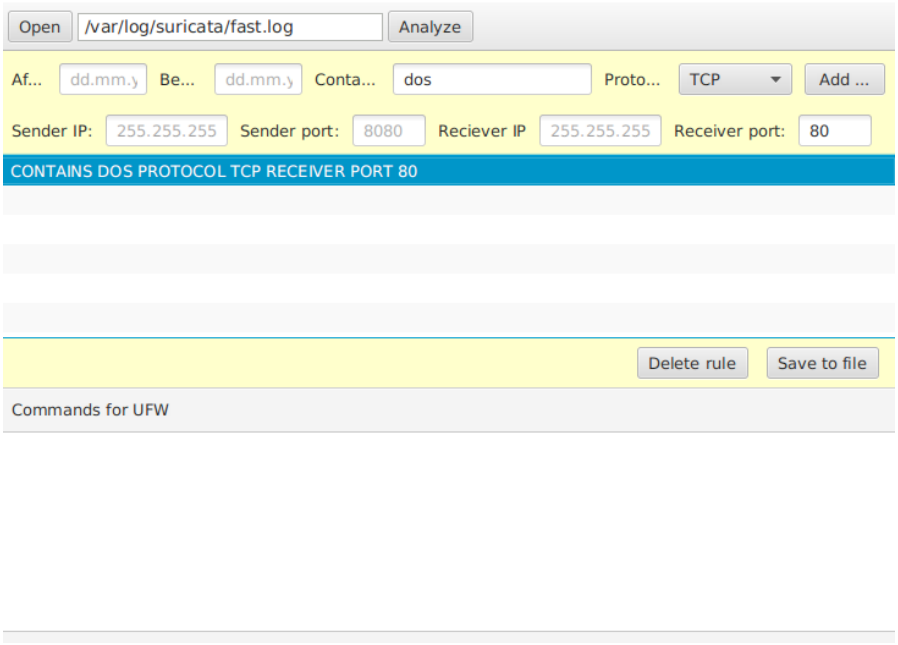

Figure 2.12 – Creating a rule for a module.

After analyzing the log file, the software module generates commands for the firewall, according to the data from the indicators that fell under the rules of the module, and displays them in the lower list (Fig. 2.13).

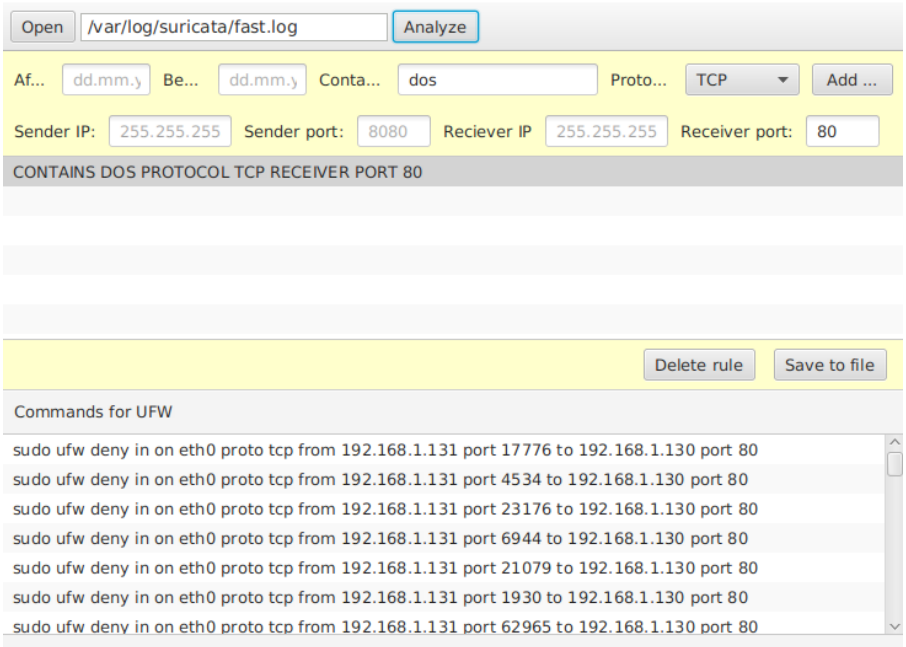

Figure 2.13 – Formed commands for the firewall.

Copy any command and run it in the terminal (Fig. 2.14).

```
administrator@ubuntu:~$ sudo ufw deny in on eth0 proto tcp from 192.168.1.131 po
rt 23176 to 192.168.1.130 port 80
[sudo] password for administrator:
Rule added
```

Figure 2.14 – Running the command in the terminal.

So, as we can see, the command was executed successfully, tcp traffic from the ip address 192.168.1.131 and port 23176, which were involved in the attack, will not pass through the network.

In this section, the algorithm of the software module is developed. The software module itself was developed and its description was created in accordance with "DSTU 3918-99). It was also tested in a virtual network. The program code of the module is given in the appendix.

3 LIFE SAFETY, BASICS OF LABOR PROTECTION

Currently, the transition to IPv6 is a topical issue for almost all ISPs, businesses and institutions, which is why the workplace of a specialist in implementing a new solution can be considered the office space of the network technology department of any company.

In this section we will consider the room in which the solution developed in this work will be used. In this room, workers may be affected by adverse conditions such as high ambient temperatures, insufficient natural or artificial lighting, increased noise levels, and interactions with electrical appliances. Based on this, it is necessary to conduct an analysis of potential hazards to workers in the room.

3.1 Basics of labor protection

3.1.1 Characteristics of the organization of production, technology in terms of labor protection

The designed room is located on the fifth floor of a ten-storey building.

Consider the plan of the room, which is shown in Figure 3.1. Table 3.1 shows the characteristics of the cabinet. Table 3.1 shows the explication of the equipment.

The room is designed for four workstations, each equipped with a computer. The plan of the room is shown in Fig. 3.1, the explication of the equipment is given in table 3.2.

The room has one window facing northeast, which provides a coefficient of natural light of 1.5%. The window consists of six rectangular sections 80 centimeters long and 330 centimeters high, with a total area of 15.84 m^2. Additionally equipped with adjustable vertical peach blinds. Workplaces are located so that the window is located to the left of the employee.

Table 3.1 – Characteristics of the cabinet

The length of the room a, m	6,325
Width of the room b, Kyiv	6
Room height h, m	3,3
Room volume V, m^3	118,8
Room area S, m^2	36
Number of employees, pers.	4
Volume of premises per 1 employee, m^3 / person	29,7
Room area per 1 employee, m^2 / person	9

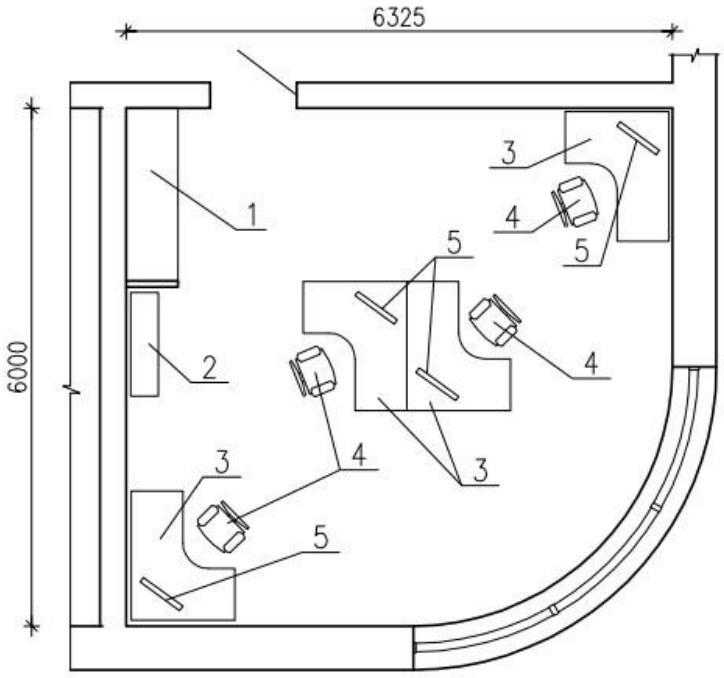

Figure 3.1 – Plan of the room

The floor in the room is flat, warm, impact resistant. An olive-colored carpet was chosen as the floor covering, which provides high sound absorption and no lint, which facilitates cleaning.

Table 3.2 – Explication of the equipment

№ поз.	Name	Overall dimensions l x b x h (см)
1	The case is built in with section for clothes	200 x 60 x 330
2	Bookcase	120 x 32 x 185
3	Office desk for computer	150 x 120 x 80
4	Swivel office chair	46 x 46 x 52/85
5	Monitor	21’

The walls of the room meet the requirements of noise and heat protection. Covered with water-emulsion paint of light olive color. Easy to clean and wash.

The ceiling is covered with white water-based paint.

Entrance doors to the office are single metal-plastic with an insert of tinted glass, have a height of 205 and a width of 90 centimeters, open into the corridor. Near the front door there is a built-in wardrobe with a clothing section 330 cm high, 200 cm wide and 60 cm deep, designed for personal belongings of employees. There is also a first aid kit in the closet. Next to it is a bookcase 185 cm high, 120 cm wide and 32 cm deep. Above the door is a "split" air conditioner (not shown).

For each employee, the workplace is equipped with a computer desk 80 cm high, 150 cm long and 120 cm wide, and a swivel chair.

The area per employee is 9 m^2 (for PC rooms, the area per employee must be at least 6.0 m^2). The volume of the room per employee is 29.7 m^3 (for rooms with a PC, the volume of the room per employee must be at least 20 m^3).

These characteristics meet the requirements of [14]. The color of the interiors meets the requirements of technical aesthetics.

3.1.2 Legislation on labor protection in the field of information technology

The Constitution of Ukraine includes among the social rights of everyone the right to health care, medical assistance and medical insurance (Article 49), appropriate, safe and healthy working conditions (Article 43). According to Article 12 of the International Covenant on Economic, Social and Cultural Rights, everyone has the right to medical care and medical treatment in the event of illness. Among the basic labor rights of employees of Art. 2 of the Labor Code of Ukraine indicates the right to healthy and safe working conditions. St. 6 of the Fundamentals of Ukrainian Legislation on Health Care enshrines the right to health care, which includes, inter alia, the right to safe and healthy working conditions.

State, public or other bodies, enterprises, institutions, organizations, officials and citizens are obliged to ensure the priority of health care in their own activities, not to harm the health of the population and individuals (Article 5 of the Fundamentals of Legislation Of Ukraine on health care). Noting the need to create safe and healthy working conditions in the process of employment, scientific and educational literature on labor law has always used the term "labor protection". The term "labor protection" is used in two senses: broad and narrow. As B.I. Prokopenko, in a broad sense, the concept of "labor protection" includes "those guarantees for workers that provide all the rules of labor law."

In a broad sense, labor protection is understood as a set of legal norms that cover the whole range of issues of labor application and belonging to various institutions of labor law (employment contract, working time and leisure time, etc.). These include rules prohibiting unjustified refusal to hire, restricting the transfer and dismissal of employees, setting working hours, regulating leisure time, and many others aimed at creating favorable general working conditions.

The term "occupational safety" in the narrow sense has always defined the creation of healthy and safe working conditions for workers. Law of Ukraine "On labor protection" of October 14, 1992 in Art. 1 defines labor protection as follows:

"Labor protection is a system of legal, socio-economic, organizational-technical and treatment-and-prophylactic measures and means aimed at preserving human health and ability to work." Based on the content of the law and other above-mentioned regulations, it is more appropriate, in our opinion, instead of the term "occupational safety" in the narrow sense to use the term "occupational health", because in fact the purpose of such measures is protection of the employee's health, preservation of his ability to work at work during the performance of duties.

Recently, health care requirements are often not met by companies of various legal forms that use the work of employees. Many business leaders

are irresponsible about their responsibilities to create healthy and safe working conditions, and often consider these issues to be secondary.

This state of health care at work is explained primarily by the difficult economic situation of the state, as well as other objective and subjective reasons, which are the depreciation of fixed assets, the fact that there is no interest of owners to improve conditions without labor incomes, incompetence of the majority of personnel in health care issues, low labor and technological discipline, insufficient role of bodies of supervision and control over observance of the legislation on labor and health care in the process of work. More than 3.4 million people work in conditions that do not meet sanitary and hygienic standards. The security of workers with personal protective equipment does not exceed 40-50%. Annual payments for compensation for damage to life and health of workers reach UAH 400 million. Of particular concern is the growing number of accidents involving group accidents.

The main directions of social policy are the need to reform the labor protection system, the main purpose of which is to significantly reduce the level of occupational injuries and diseases, reduce the factors of harmful effects on workers and release workers from harmful and difficult working conditions. Although the main term uses the traditional term "labor protection", but in fact it is about the health and ability to work of workers.

To this end, it is envisaged: to complete the formation of the system of labor protection management at the regional and industrial levels for enterprises, institutions, organizations of all forms of ownership, activities; to review legislation and regulations on labor protection, taking into account the requirements of regulations of the European Union; to adopt legislative acts on high-risk facilities and on the safety of industrial products; to move to the territorial and sectoral principle of state supervision of health care in the labor process; ensure stable financing of health care measures, etc. Unfortunately, some of these measures remain on paper.

The most important norms on health protection of workers at work are enshrined in the Law of Ukraine "On Labor Protection" of October 14, 1992, in three chapters of the Labor Code (Chapter XI "Labor Protection", Chapter XII "Women's Labor", Chapter XIII "Youth Labor"). "), as well as in bylaws – regulations, rules, instructions, acts of social partnership, local regulations.

3.2 Life safety

3.2.1 Analysis of harmful and dangerous factors

Microclimatic conditions

Sanitary and hygienic standardization of microclimate conditions is carried out according to [15], which establish the optimal and permissible parameters of the microclimate depending on the total energy consumption of the organism during the work and the period of the year.

The work performed by the staff belongs to the physical work of the category "Light Ia" according to [15]. The optimal values of the microclimate characteristics are given in table 3.3.

Table 3.3 – Optimal microclimate indicators

Period of year Air temperature	° C Relative humidity	% Air velocity	m / s
Cold period of the year	22–24	60–40	0.1
Warm period of the year	23–25	60–40	0.1

The temperature of the internal surfaces of the working area (walls, floor, ceiling) of technological equipment (screens, etc.), external surfaces of the equipment should not exceed 2 °C beyond the optimum air temperatures for this category of work.

Air conditioning is used to maintain a favorable microclimate. For the designed room, the approximate power of the "split" air conditioner is – 5.8 kW. HITACHI RAS-18LH2 / RAC-18LH1 with the following characteristics meets this requirement:

– operating temperature range: from −10 °C to + 43 °C;
– cooling capacity: 4.89 – 4.91 kW;
– heat output: 5.70 – 5.72 kW;
– noise level during cooling (high / mid / low): 45/42/39/36 dB (A);
– noise level during heating (high / Wed / Low): 43/39/36/36 dB (A).

In the cold period of the year, in order to maintain a favorable microclimate, heating is provided from the roof boiler house located above the technical floor of the building. The heating system is two-pipe, with the top dilution of the heat carrier. Heating devices – Purmo panel radiators. To regulate the heat flow from the heater, a control valve with a thermostatic head is installed on the coolant line to the appliance.

Industrial lighting

Lighting in the office natural side and artificial general.

Lateral natural lighting should be provided through light slots oriented mainly to the north or northeast and provide a natural light factor (KPI) of 1.5% according to [16].

According to [16], the work performed in the room is classified as medium accuracy – work is performed with objects of recognition 0.5 mm-1 mm. The level of illumination in the workplace should be at least 300 lux.

Protection against industrial noise

Sources of noise in the room are computer cooling fans (maximum noise level – 35 dBA) and "split" air conditioner (maximum noise level – 45 dBA). Sound can be considered constant, as its level during the working day changes by no more than 5 dBA.

The allowable equivalent sound level according to [17] is as follows: for a computer programmer, the normalized sound pressure must not exceed 50 dBA. In this case, the total sound pressure level does not exceed the normalized value.

Protection against electromagnetic fields

The source of electrostatic field and electromagnetic radiation in a wide range of frequencies (over 50 Hz and infrared, radio frequency, infrared, visible, ultraviolet, X-ray) are personal computers.

3.2.2 Engineering solution

Calculate the level of lighting in the room. Artificial lighting should be carried out by means of 9 two-lamp lamps of the LD type placed in three rows from the FL40W / 635 lamp, with a power of 40 W, and a luminous flux of 2800 lm.

Figure 3.2 shows the plan of the room, taking into account the lighting system.

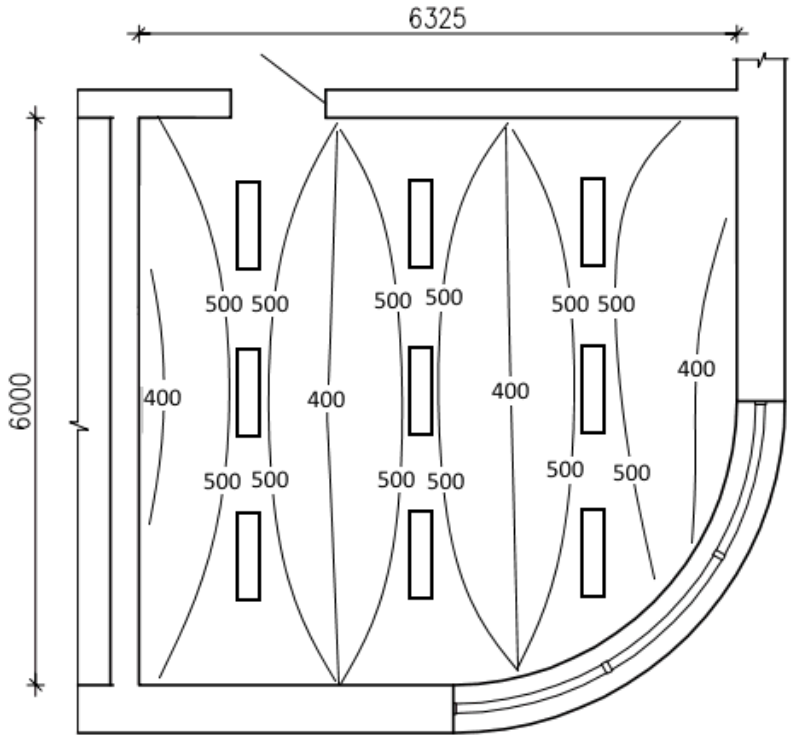

Figure 3.2 – Plan of the room with lighting

DIALux 4.9 software with a plug-in for Philips lighting systems was used to calculate indoor lighting.

Such artificial lighting will create an illumination of 381 lux and this value corresponds to the norm.

3.2.3 Electrical safety

According to [18], the degree of danger of electric shock to the room refers to the room without increased danger. The room has a 3-phase power supply with a voltage of 220 V, a frequency of 50 Hz and a maximum current of 32 A. Electricity consumers are four personal computers, air conditioning and lighting.

The mains is made of three conductors – phase, neutral, protective earthing conductor, which are conducted in the floor near the walls of the room, in flexible metal sleeves with taps up to four groups of sockets.

The use of a neutral conductor as a neutral protective conductor is prohibited, and it is not permissible to connect these conductors on the shield to a single contact terminal.

The building has a protective earthing, which is designed to protect people from electric shock and grounding of the lightning protection system, which serves to divert lightning current and protect equipment from lightning.

A group shield located in the room to which electrical installations, cables and wires with copper cores with a section diameter of at least 2.5 mm^2 are connected must be used.

The following technical protective measures of electrical safety must be carried out: working insulation of live parts and plastic boxes made of flame-retardant materials with moderate smoke-generating capacity. When connecting the electrical connector to the mains, the connection of the housing to the ground must be guaranteed. All electrical outlets must be marked with voltage.

3.2.4 Fire safety

The main causes that can lead to a fire in the room are: faults in electrical equipment – electrical insulation; malfunctions caused by mechanical damage, etc .; malfunctions in computer technology, for example, short circuit, violation of the fire regime.

Items and materials that can burn: furniture – tables, chairs, cabinets, etc .; paper – documentation, structural elements of the room – floor coverings, doors, window frames, structural elements of PCs and peripherals – printer cases, monitors, keyboards, etc.

According to [19], the premises belong to category "B" of fire safety, as it contains flammable materials such as paper and wood and no explosive materials.

Combined fire alarm sensors are installed in the room for timely fire warning. You can use the ACU-100 sensor, which signals an alarm after detecting visible smoke (optical sensor) or after registering a high temperature (thermal

sensor). The thermal sensor responds to exceeding the threshold temperature and its growth rate. The sensor transmits an alarm signal until its cause is eliminated (smoke, high temperature). In case of system operation, the signal should arrive to the next in the case.

According to [20], 2 fire extinguishers are installed in the room for every 20 m^2. The distance between the locations of fire extinguishers should not exceed 15 m. There are four carbon dioxide-bromoethyl fire extinguishers type VVB-3, which are suitable for extinguishing small sources of ignition, as well as electrical equipment up to 380V. Fire extinguishers work effectively at temperatures from –60 to +55 ° C.

CONCLUSION

The main types of network attacks and the prerequisites for the use of intrusion detection systems and the creation of a SOC, as effective in countering network attacks, their properties and the principle of operation are considered in detail.

The topic of the diploma project is the software module of the cyber security event management system. The goal of the dialom work is to create a software module that automates the process of forming commands for the IPS (Firewall) actuator. This module will allow timely and quick detection of an information attack based on records from IDS sensors and the implementation of measures aimed at preventing it in the future.

During the development of the diploma project, the area of information security in computer networks was considered - the types and mechanics of network attacks, malicious software, intrusion detection systems and modern APT attacks were described in detail. The software module was developed on the basis of the Suricata intrusion detection system, implemented software elements for creating commands to IPS indicators, in our case Firewall, using the Java 8 language.

REFERENCES

1. Information systems and technologies in management / http://pidruchniki.com/74225/informatika/avtomatizovani_sistemi_upravlinnya_obroblennya_analizu_informatsiyi.

2. Analysis of modern intrusion detection systems / O.V. Severinov, A.G. Hryenov, 2016. 16 p.

3. Protected operating systems / Lviv Polytechnic National University, BICS department Lecture 3, 2016.

4. UFW / http://integrator.adior.ru/index.php/linux–command/364–ufw–firewall–linux–pomogayushchij–upravlyat–iptables.

5. Comparison of programming languages / http://lib.mdpu.org.ua/e–book/vstup/L4.html

6. Network equipment - devices that make up a computer network / http://ittexnoall.com/index.php/osnovy–kompyutera/1002–merezheve–obladnannya–pristroji–z–yakikh–skladaetsya–komp–yuterna–merezha.html

7. Characteristics of programming languages / Essay "Possibilities and Purpose of the Language for Creating Server Scripts" Ph.D. S.V. Lenkov, 2015 3–4 p.