УДК 002:004.056
https://doi.org/10.47533/2024.1606-146X.50

G. JUSSUPBEKOVA[1], ZH. IZTAYEV[1], G. ORDABAYEVA[2,3], A.KYDYRBEKOVA[1], N. RAKHYMBEK[1]*

[1]M. Auezov South Kazakhstan University, Shymkent, Kazakhstan;
[2]Al-Farabi Kazakh National University, Almaty, Kazakhstan;
[3]Kazakh National Agrarian Research University, Almaty, Kazakhstan.
**E-mail: gulzat20.10@mail.ru*

THE METHODS AND TOOLS OF ENSURING INFORMATION SECURITY OF NETWORKS

Gulzat Tursbekovna Jussupbekova – Candidate of Pedagogical Sciences, Head of the Department of Information and Communication Technologies, M. Auezov South Kazakhstan University, Shymkent, Kazakhstan;

E-mail: gulzat20.10@mail.ru, https://orcid.org/0000-0003-1727-0966

Zhalgasbek Dulatovich Iztayev – Candidate of Pedagogical Sciences, Head of the Department of Information Systems and Modeling, M. Auezov South Kazakhstan University, Shymkent, Kazakhstan;

E-mail: Zhalgasbek71@mail.ru, https://orcid.org/0000-0002-3210-2963

Gulzinat Koishymanovna Ordabaeva – senior lecturer, Department of Information Systems, Al-Farabi Kazakh National University, Almaty, Kazakhstan;

E-mail: gulzi200988@mail.ru, https://orcid.org/0000-0001-9952-1620

Aizat Siyazbekovna Kydyrbekova – senior lecturer, Department of Computer Engineering and Software, M. Auezov South Kazakhstan University, Shymkent, Kazakhstan;

E-mail: *kas.aizat@mail.ru*; https://orcid.org/0000-0001-5740-4100

Nazira Zhaylauovna Rakhymbek – senior lecturer, Department of Information Technologies, M. Auezov South Kazakhstan University, Shymkent, Kazakhstan.

E-mail: naziki_jan00@mail.ru, https://orcid.org/0000-0003-4229-2286

Currently, there is an increase in the number of information threats that lead to unstable operation of data networks. This is due to the mass use, the complication of the hierarchy of area networks, the increase in the heterogeneity of software tools, and the complication of the functionality of network services. In such cases, the development and improvement of methods for determining information security in data transmission networks has a great importance. The article discusses ways to increase the information security of the data network by increasing the reliability of detecting deviations in the operation of the main nodes of the data network and reducing the number of false starts when automating the detection of threats.

Experimental verification and evaluation of the effectiveness of the methods were considered, it was shown that the developed methods allow skipping the anomaly of the first type and minimizing errors of the second type. The methods were implemented software in the form of a prototype access detection system (ADS).

Keywords: *data transmission network, network statistics, information security, access detection system, operating system.*

Г. ДЖУСУПБЕКОВА[1*], Ж.Д. ИЗТАЕВ[1], Г. ОРДАБАЕВА[2,3],
А.КЫДЫРБЕКОВА[1], Н. РАХЫМБЕК[1]

[1]М. Әуезов атындағы Оңтүстік Қазақстан университеті, Шымкент, Қазақстан;
[2]әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан;
[3]Қазақ ұлттық аграрлық зерттеу университеті, Алматы, Қазақстан.
**E-mail: gulzat20.10@mail.ru*

ЖЕЛІЛЕРДІҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІ МЕН ҚҰРАЛДАРЫ

Джусупбекова Гулзат Турысбековна – педагогика ғылымдарының кандидаты, «Ақпараттық-коммуникациялық технологиялар» кафедрасының меңгерушісі, М.Ауэзов атындағы Оңтүстік Қазақстан университеті, Шымкент, Қазақстан;

E-mail: gulzat20.10@mail.ru, https://orcid.org/0000-0003-1727-0966

Жалғасбек Дулатович Изтаев – педагогика ғылымдарының кандидаты, «Ақпараттық жүйелер мен модельдеу» кафедрасының меңгерушісі, М.Ауэзов атындағы Оңтүстік Қазақстан университеті, Шымкент, ;

E-mail: Zhalgasbek71@mail.ru, https://orcid.org/0000-0002-3210-2963

Ордабаева Гулзинат Койшымановна – «Ақпараттық жүйелер» кафедрасының аға оқытушысы, әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан;

E-mail: gulzi200988@mail.ru, https://orcid.org/0000-0001-9952-1620

Айзат Сиязбекқызы Қыдырбекова – «Есептеу техникасы және бағдарламалық қамтамасыз ету» кафедрасының аға оқытушысы, М.Ауэзов атындағы Оңтүстік Қазақстан университеті, Шымкент, Қазақстан;

E-mail: kas.aizat@mail.ru; https://orcid.org/0000-0001-5740-4100

Назира Жайлауовна Рахымбек – «Ақпараттық-коммуникациялық технологиялар» кафедрасының аға оқытушысы, М.Ауэзов атындағы Оңтүстік Қазақстан университеті, Шымкент, Қазақстан;

E-mail: naziki_jan00@mail.ru, https://orcid.org/0000-0003-4229-2286

Қазіргі уақытта деректер желілерінің тұрақсыз жұмыс істеуіне әкелетін ақпараттық қауіптер санының өсуі байқалады. Бұл жаппай қолдану, есептеу желілерінің иерархиясының күрделенуі, программалық құралдардың гетерогенділігінің артуы, желілік қызметтердің функционалдығының күрделенуі себептерінен болып табылады. Мұндай жағдайларда деректерді беру желілерінде ақпараттық қауіпсіздікті анықтау әдістерін әзірлеу және жетілдіру үлкен маңызға ие. Мақалада деректер желісінің негізгі түйіндерінің жұмысындағы ауытқуларды анықтаудың сенімділігін арттыру және қатерлерді анықтауды автоматтандыру кезінде жалған іске қосулардың санын азайту арқылы деректер желісінің ақпараттық қауіпсіздігін жоғарылату жолдары қарастырылған.

Әдістердің тиімділігін эксперименттік тексеру және бағалау қарастырылды, әзірленген әдістер бірінші типтегі аномалияны өткізіп жіберу және екінші типтегі қателерді азайтуға мүмкіндік беретіні көрсетілген. Әдістерді кіруді анықтау жүйесі (КАЖ) прототипі түрінде бағдарламалық қамтамасыз ету жүзеге асырылды.

Түйін сөздер: *деректерді беру желілері, желілік статистика, ақпараттық қауіпсіздік, кіруді анықтау жүйесі, операциялық жүйе.*

Г. ДЖУСУПБЕКОВА[1*], Ж.Д. ИЗТАЕВ[1], Г. ОРДАБАЕВА[2,3], А.КЫДЫРБЕКОВА[1], Н. РАХЫМБЕК[1]

[1]Южно-Казахстанский университет имени М.Ауэзова, Шымкент, Казахстан;
[2]Казахский национальный университет имени аль-Фараби, Алматы, Казахстан;
[3]Казахский национальный аграрный исследовательский университет, Алматы, Казахстан.
**E-mail: gulzat20.10@mail.ru*

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТЕЙ

Джусупбекова Гулзат Турысбековна – кандидат педагогических наук, зав. кафедрой «Информационно-коммуникационные технологии», Южно-Казахстанский университет имени М.Ауэзова, Шымкент, Казахстан;

E-mail: gulzat20.10@mail.ru, https://orcid.org/0000-0003-1727-0966

Жалғасбек Дулатович Изтаев – кандидат педагогических наук, зав. кафедрой «Информационные системы и моделирование», Южно-Казахстанский университет имени М.Ауэзова, Шымкент, Казахстан;

E-mail: Zhalgasbek71@mail.ru, https://orcid.org/0000-0002-3210-2963

Ордабаева Гулзинат Койшымановна – ст.преп. кафедры «Информационные системы», Казахский национальный университет имени аль-Фараби, Алматы, Казахстан;

E-mail: gulzi200988@mail.ru, https://orcid.org/0000-0001-9952-1620

Кыдырбекова Айзат Сиязбековна – магистрант, ст.преподаватель кафедры «Вычислительная техника и программное обеспечение», Южно-Казахстанский университет им. М.Ауезова, Шымкент, Казахстан;

E-mail: kas.aizat@mail.ru; https://orcid.org/0000-0001-5740-4100

Назира Жайлауовна Рахымбек – ст.преп. кафедры «Информационные технологий», Южно-Казахстанский университет имени М.Ауэзова, Шымкент, Казахстан.

E-mail: naziki_jan00@mail.ru, https://orcid.org/0000-0003-4229-2286

В настоящее время наблюдается рост информационных угроз, приводящих к неустойчивому функционированию сетей передачи данных. Это вызвано массовым применением, усложнением иерархии вычислительных сетей, увеличением неоднородности программных средств, усложнением функционала сетевых сервисов. В таких случаях большое значение имеет разработка и совершенствование методов определения информационной безопасности в сетях передачи данных. В статье рассмотрены пути повышения информационной безопасности сети передачи данных путем повышения надежности обнаружения отклонений в работе основных узлов сети передачи данных и уменьшения количества ложных срабатываний при автоматизации обнаружения угроз.

Рассмотрена экспериментальная проверка и оценка эффективности методов, показано, что разработанные методы позволяют пропускать аномалии первого типа и минимизировать ошибки второго типа. Реализовано программное обеспечение в виде прототипа системы обнаружения вторжений (СОВ).

Ключевые слова: *сети передачи данных, сетевая статистика, информационная безопасность, система обнаружения вторжений, операционная система.*

Introduction. Currently, there is an increase in the number of information threats and factors leading to the unstable operation of data transmission network (DTN). The prerequisites for this growth are mass use, the complication of the hierarchy of area networks and an increase in their structural complexity, an increase in the heterogeneity of software and hardware, the complication of the functionality of network services, which leads to the emergence of various vulnerabilities. In such cases, the development and improvement of methods for detecting information threats in the DTN has a great importance. One of the components of ensuring information protection of networks is software complexes for detecting malicious or suspicious activity - an access detection system (ADS). Access detection systems solve the problems of detecting deviations in the operation of the main nodes of the DTN.

Anomalies are defined as deviations from the normal operating mode, in particular, changes in the performance indicators of DTN components. Examples of performance indicators includes the number of packets or bytes received or sent by a hardware port per unit of time, the number of discarded incoming or outgoing packets per unit of time, processor load, etc.

Theoretical and practical developments implemented in closed solutions of leading manufacturers of network equipment (Cisco, Juniper, Huawei) have limited use due to the high cost and complexity of integration, while open products have disadvantages that do not allow solving the problems of timely and reliable detection of deviations. Also, taking into account the growing publication activity in this area, the development of methods and tools for detecting anomalies should be recognized as an urgent task from a scientific and practical point of view.

Research methodology and results. Information Security is a state of the information field in which accidental or intentional interception, decoding and decoding of the source information field, its unauthorized use and copying, the introduction of third-party information flows into the information field is excluded, which leads to distortion or its violation [1].

Security of data transmission networks-protection against unauthorized use of the DTN, which leads to changes, disclosure or destruction of the DTN structure, functional properties of the DTN, or data transmitted to the DTN. The task of ensuring the information security of a DTN should be solved in a comprehensive manner depending on the following circumstances:

1) a network is a set of software and hardware programs that interact with each other and created according to different standards from different manufacturers, that is, a computing environment with high heterogeneity. The specificity of each network element must be taken into account when designing a Network Security Management System;

2) network communication is carried out through protocols belonging to a specific network stack, such as TSP/IP or OSI. At each level, it is necessary to ensure reliable protection of transmitted data;

3) the presence of heterogeneous defense mechanisms in the network, their mutual influence and impact on the operation of the network should be carefully studied. The operation of different security subsystems must be coordinated, however, in practice it is not always achieved;

4) when designing a defense system, it is necessary to pay attention to the statistics of threats and take into account the possibility of arising of possible (unknown) threats that can occur.

A network attack is an implemented information threat, that is, a destructive impact on the information system through the DTN.

In order to successfully counter DTN attacks (the purpose of the attacks can be both the hardware itself controlled by the DTNs and the resources available through the DTNs), it is necessary to obtain information about the operation of the DTNs components. DTNs components are understood as the main nodes of the computing network - switches, routers, servers, PABX and also other active telecommunications equipment. In some cases, DTNs components can be considered as software systemssuch as a web server application or an ONSR server application. Obtaining information is achieved by monitoring the components of the DTN. Data on the operation of equipment and information systems will be available for analysis in the form of performance indicators - temporary series of values characterizing a certain aspect of the operation of the DTNs component. Monitoring of information flows in a DTNs is an important part of the process of ensuring information security in a DTN. To detect and prevent network attacks, special software complexes are used, that is, systems for detecting and preventing attacks.

ADS is a software or hardware tool that detects information threats in computing systems and data networks. Intrusion Detection System (IDS) are the main element of the network protection complex.

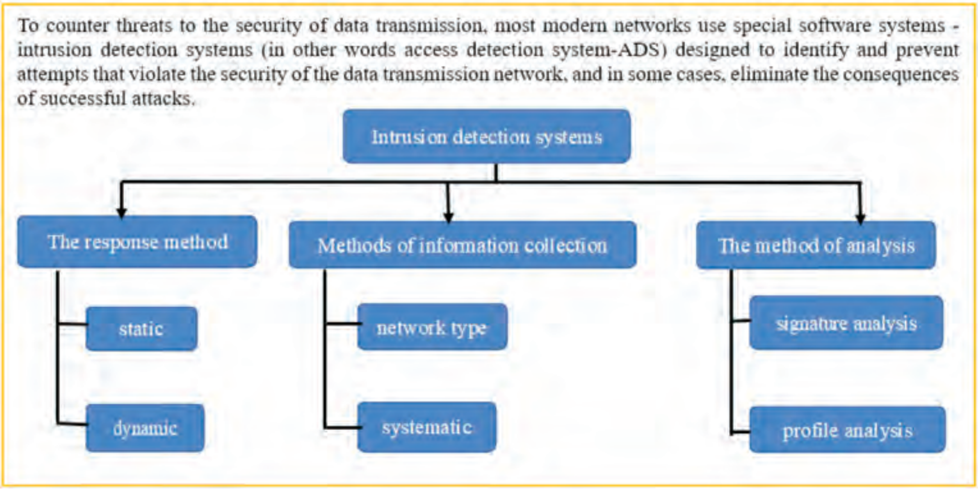
In the work of Kornienko and Slusarenko "Systems and methods of detection of intrusions: current state and directions of improvement", ADS were defined as systems that collect information from various points of a protected computer system (computing network) and analyze information on the axis, which, in violation actions, also detect specific protective (intrusion) violations [2, 3].

Basically, the ADS architecture includes:

1) a sensor subsystem for collecting information (events related to the security of the protected system);

2) a data storage subsystem for long-term storage of the collected data and analysis results;

3) an analysis subsystem for detecting attacks and suspicious activity based on obtained statistics on the operation of a computing system or DTN (Figure 1).



To counter threats to the security of data transmission, most modern networks use special software systems - intrusion detection systems (in other words access detection system-ADS) designed to identify and prevent attempts that violate the security of the data transmission network, and in some cases, eliminate the consequences of successful attacks.

Figure 1 – Methods of access detection system

The concept of intrusion detection systems (ADS-access detection system) was first formulated by D. Anderson in an article devoted to methods and tools of monitoring area networks [3]. In 1986, D. Denning published an article describing the ADS model, which laid the foundation for most modern systems. In this model, it was proposed to use statistical methods to determine the entry. The development was called IDES (Intrusion detection expert system) and was close in functionality to expert systems, as it did not include instant data analysis. The system analyzed both network traffic and user application data. The expert system contained data to detect known anomalies and network attacks. The system also had an analysis module based on statistical methods. T. Lunt proposed using a neural network to increase the efficiency of detecting anomalies, introduced as a prototype in 1993.

In 1988, the MIDAS (Multics intrusion detection and alert system) was developed, the core of which is an Expert System written in LISP, which made it possible to add any complex detection rules. The development of intrusion detection systems using operational analysis did not stop: in 1988, haystack ADS was developed, in 1989, W&S (Wisdom & Sense), which used an approach to detecting deviations based on statistical methods [4].

Systems that use a statistical approach to data analysis include Distributed intrusion detection system (DIDS) and Network anomaly detection and intrusion reporter (NADIR).

Network statistics analysis and abuse and invasion detection systems have often been developed as an addition to the network firewall or as a component of it. This is considered in a number of systems that use the libpcar library to capture traffic passing through a network node with a unix-like OS (WGO, NFR, Snort).

Products from leading network equipment manufacturers are always tied to a hardware platform and are almost always part of a hardware firewall (firewall) [5].

Network monitoring organization is the process of installing and configuring infrastructure for continuous monitoring of network devices and traffic in order to detect anomalies and ensure high network availability and performance. There are several basic steps for organizing network monitoring:

1) defining control goals: we define the goals of network monitoring. This may include network fault detection and prevention, performance monitoring, anomaly detection, resource usage monitoring and other options important to the network;

2) selection of appropriate monitoring tools: explore the various monitoring tools available on the market and choose the ones that best suit your needs. These can be commercial or free tools such as Nagios, Zabbix, PRTG, Prometheus and others;

3) deployment of monitoring infrastructure: install and configure selected monitoring tools on the network. This usually involves setting up a monitoring server, setting up agents or sensors on monitored devices, and configuring alerts and reports;

4) determining monitored parameters: determine the parameters and dimensions you want to monitor on the network. These can be the status of devices, bandwidth

usage, delays, errors, packet losses, and other indicators specific to the network infrastructure;

5) setting alerts and alarms: set up a system of alerts and alarms to be aware of any abnormalities or problems in the network. Specify the contacts from which notifications will be received and identify the most important levels at which alarms will appear;

6) analyze and respond: constantly analyze the monitoring data and respond to the identified problems. Use the information obtained to optimize the network infrastructure, prevent failures, and take steps to improve performance;

7) scale and upgrade: scale the monitoring infrastructure by adding new devices and monitoring options if necessary. Update your tracking tools regularly to use the latest features and bug fixes. [6].

An important aspect of ADS operation is the technology of monitoring the components of the DTN used in it. The organization of monitoring of DTNs components is a complex task that must be solved in a comprehensive manner. The general direction of development of network technologies raises important questions regarding the management of DTN. Control over the network, including the operation of network equipment, activity of users and applications will increase.

DTN can have a number of structural and functional features, depending on the field of application. Most DTN, which are part of large networks, are local area computing networks (LANs) created using Ethernet technology. In a modern local area network of an enterprise or last mile provider, three levels can be distinguished:

1) access level (access layer);

2) distribution layer (distribution layer);

3) network core (core).

Entry-level switches provide ports to last users (speeds ranging from 10 Mbps to 1 Gbit/s), forming virtual LANs. Connections between the access level and the distribution level can be made by Gigabit Ethernet or 10 Gigabit Ethernet channel.

Distribution level switches connect the second level blocks (residential areas, districts) through high-speed channels to the core, which includes the ADS L3 network with switching. At the kernellevel, external traffic routing, shaping, network address translation, filtering and traffic accounting are carried out. Several logical levels can be combined on one physical device, such as Access/Distribution or Distribution/Core [7].

Network monitoring is a specially organized systematic control of the state of computing network objects, evaluation of the phenomena and processes occurring in the network, control or prediction.

The main monitoring methods are presented and their advantages and disadvantages are shown in Table 1.

Currently, Simple Network Management Protocol (SNMP) is supported by most of the active network equipment and even some software complexes. It is not an international standard, unlike the SMR protocol, and is specified in the RFC series, the main ones being RFC 3411-3418 and 6353 [8].

Table 1 – Advantages and disadvantages of basic monitoring methods [7]

Monitoring	Advantages	Disadvantages
On the basis of SNMP	Many of network devices are supported, many of indicators	The possibility of packet loss, the difficulty of conducting survey on many of the devices on a short survey interval
On the basis of NetFlow, sFlow, jFlow, NetStream	Many of the network devices are supported	The possibility of packet loss, the information is not stored on the monitoring object after it is sent to the collector
Analysis of network packets	Detailed analysis of events and ability to rebuild	High load on the system, limited selection of the network components – control objects
Monitoring network stack events	Less load on the system in comparison with network packet interception	Limited selection of the network components - control objects, implementation depends on the capabilities of Operation System
By making control (on the basis of ICMP, UDP, TCP)	Relative ease of implementation	Limited set of OS network performance indicators (depends on the time of delivery of the packets)
Application tool (ARM, AIC)	Detailed analysis of events and evaluation of the full response time of applications (end-to-end response time)	High labor intensity, do not use (switch, router) in closed device
Analysis of journals (syslog, iptables)	Relative ease of implementation	Limited set of performance indicators (mostly signature suitable for analysis)

Agents work on network nodes and collect information about the operation of these nodes. The manager interacts with agents using the SNMP protocol for the purpose of exchanging management information. As a rule, the interaction is carried out by the manager of many agents in the form of a periodic survey (Table 2).

Table 2 – Basic operations of the SNMP protocol

Operation	Minimum version of the protocol	Description
Get-Request	1	Request for a variable
Get-Next-Request	1	Request for a next variable in the table
Get-Bulk-Request	2	Request for a variables in OID tree branch
Response	1	Agent response
Set-Request	1	Write a variable
Trap	1	Trap manager agent message about a change in a variable
In form-Request	2	Exchange of managing information main information

SNMP message contains SNMP version number, Security Information, and a protocol block of PDU data describing the operation being performed and its parameters. To send SNMP messages, the UDP protocol is usually used (port 161). Port 162 is used to transmit data through Trap operations, which allows agents to inform the manager asynchronously about a limited number of important events. To study LDS components, the libsnmp open library and the net-snmp package were used in this work.

Since the method of searching for signatures in telecommunication data allows you to detect only known attacks, data analysis for hidden patterns, abuse and abnormal behavior of DTNs components are arises a great interest. Fluctuations in the time series of performance indicators of DTNs components are not necessarily signs of an attack or its consequences, but in most cases indicate significant changes in the DTN and can be the key to understanding by network engineers and network security specialists of the processes taking place in the DTN [9].

The main idea of any methods for detecting anomalies is to find abnormal behavior of the indicator and differences from normal. To characterize the normal behavior of the indicator, various methods and models can be used, the main ones relate to the detection of deviations in telecommunication data:

1) Markov models;
2) simulation modeling;
3) data mining;
4) fractal analysis;
5) time series analysis;
6) spectral analysis;
7) spectral-time analysis.

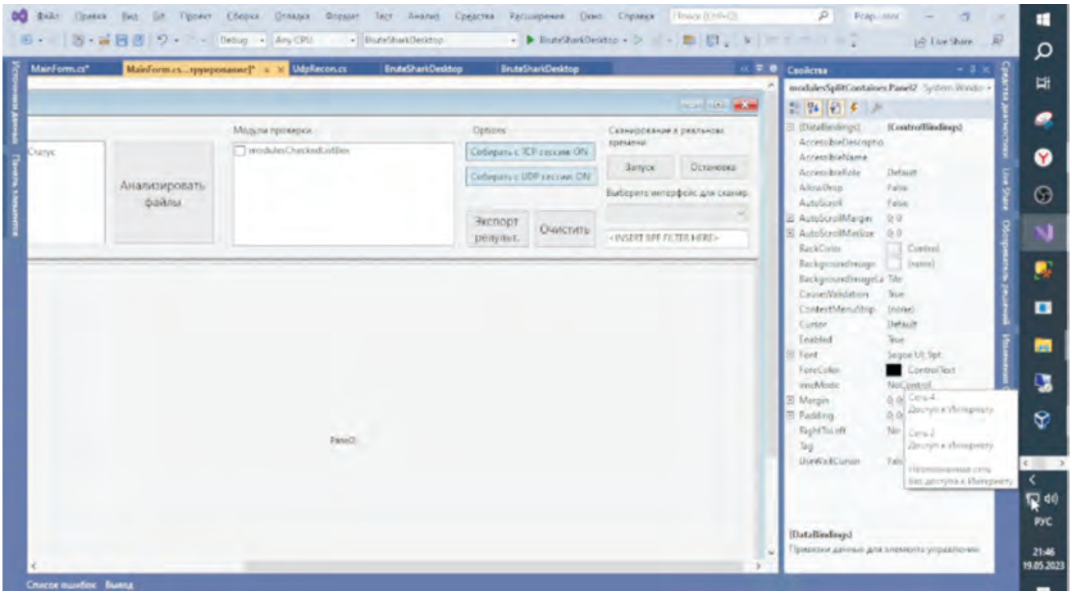
Modeling tools allow you to achieve accurate results, but creating and configuring the model requires significant computational resources and time. There are special tools for simulating the processes that take place in data networks, in particular Network Simulator 2 (NS2). Taking into account the current state of the field of research, publications on the problems of detecting network attacks and anomalies, and the functionality of software products presented on the market, we list the main directions for improving ADS:

- increasing the reliability of detecting anomalies by increasing the number of true positive rate and reducing the number of false positive rate;
- optimizing the system of training process, moving to «teacher-free»methods;
- classifying anomalies by type and identifying new types of anomalies;
- parametric detection of anomalies and network attacks;
- performing a risk assessment of detected deviations, act in accordance with the level of danger, making decisions on ways to counter threats;
- analyze the interrelated characteristics of monitoring objects and determine the relationship of characteristics. Identification of hidden patterns in data flows;
- analysis of incomplete telecommunications data flows, identification of deviations in the level of access at which processes do not determine obvious periodicity.

It should be noted that the technological problems that arise during the development of ADS remain relevant: with an increase in the computing load, the load on the network (increasing the share of Service traffic) and an increase in the number of analyzed indicators, the required amount of data storage, the distribution of the computing load on several hosts and the management of distributed system components, the availability and portability of the necessary libraries, etc.

Also, in many companies the monitoring system is included and this companies are using DTN, it means that collection of information and the storage of information about the operation of DTNs components is arrranged well. And also in many companies ADS signature is included. Unfortunately, the presence of ADS, which detects anomalies in telecommunications data streams, it is exotic. However, as mentioned above, there is an objective need to identify deviations and analyze network security events [10]. The rationale for the approach to detecting an anomaly should include logical arguments supported by evidence and relevant research. This will help establish trust in the chosen approach and confirm its effectiveness to solve a specific problem of detecting deviations. A simple way to detect anomalies is, for example, the one implemented in ProLAN products. In the interpretation of the developers of the products of this company, the assessment of the so-called «health» of the network is reduced to monitoring the limits of some indicators of the operation of switches: availability by SNMP, CPU loading, response delay by ICMP (ping), loading device ports, the number of errors in ports, the number of broadcast packets sent from the device port [11].

In the experimental part, a network traffic analyzer developed on the basis of Visual Studio was used. The program is so supportive when performing network analysis or increasing network security. The program is written in C#, supports Visual Studio 2019 or 2022 (Figure 2).

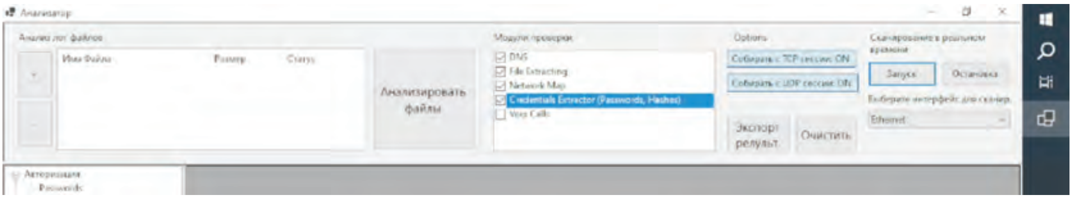


(DataBindings) (ControlBindings)
AccessibleDescriptio
AccessibleName
AccessibleRole Default
AllowDrop False
AutoScroll False
AutoScrollMargin 0; 0
AutoScrollMinSize 0; 0
BackColor Control
BackgroundImage (нет)
BackgroundImageLa Tile
CausesValidation True
ContextMenuStrip (нет)
Cursor Default
Enabled True
Font Segoe UI; 9pt
ForeColor ControlText
imeMode NoControl
Margin 0; 0
Padding 0; 0
RightToLeft No
Tag
UseWaitCursor False

(DataBindings)
Привязки данных для элемента управления

Figure 2 – Available channels (networks) list

In the next step, we select the necessary verification modules (DNS, File extraction, Network Map, Credentials Extractor) and start scanning the network (Figure 3):



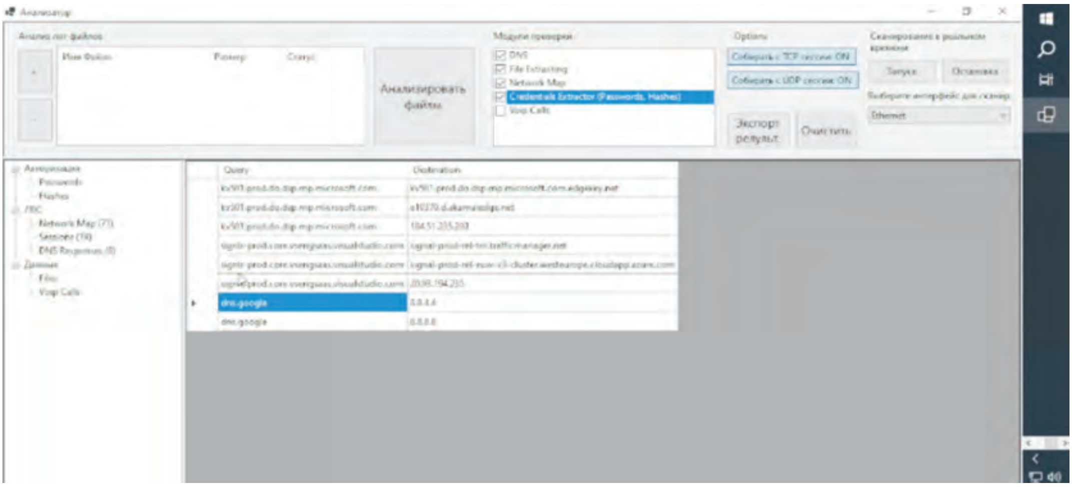
☑ DNS
☑ File Extracting
☑ Network Map
☑ Credentials Extractor (Passwords, Hashes)
□ Voip Calls

Собирать с TCP сессии ON
Собирать с UDP сессии ON

Выберите интерфейс для сканир.: Ethernet

Figure 3 – Select the necessary verification modules

On an experimental basis, Youtube network access was performed and data changes were tracked (Figure 4).



☑ DNS
☑ File Extracting
☑ Network Map
☑ Credentials Extractor (Passwords, Hashes)
□ Voip Calls

Собирать с TCP сессии ON
Собирать с UDP сессии ON

Выберите интерфейс для сканир.: Ethernet

Query	Destination
kv501.prod.do.dsp.mp.microsoft.com	kv501.prod.do.dsp.mp.microsoft.com.edgekey.net
kv501.prod.do.dsp.mp.microsoft.com	e10370.d.akamaiedge.net
kv501.prod.do.dsp.mp.microsoft.com	184.51.235.203
signalr-prod.core.vsengsaas.visualstudio.com	signal-prod-rel-tm.trafficmanager.net
signalr-prod.core.vsengsaas.visualstudio.com	signal-prod-rel-euw-c3-cluster.westeurope.cloudapp.azure.com
signalr-prod.core.vsengsaas.visualstudio.com	20.98.194.235
dns.google	8.8.4.4
dns.google	8.8.8.8

Figure 4 – There are given DND responses based on YouTube network.

When creating access detection systems, the use of the proposed methods in the software modules developed on their basis will solve the problems of timely and reliable detection of anomalies in the operation of data transmission network components. This is automates the detection of information threats and information security in data transmission networks will be increased and will be arranged more efficient work of system administrators and network security specialists.

The prototype of intrusion detection systems makes it possible to test the developed methods that has arranged for detecting anomalies and forming the profile and makes it possible to use the methods in order to apply approaches to implementing various subsystems of intrusion detection systems and to assess the complexity of implementing methods for detecting intrusions. In addition, the developed prototype of access detection systems made it possible to identify limitations and unsuccessful technical solutions in the implementation of various subsystems, which should be taken into account when creating full-fledged access detection systems.

The article developed a subsystem for recording anomalies. The anomaly registration subsystem stores event information in the system configuration database and provides the transfer of information to the web interface.

The use of the methods proposed in the software modules developed on their basis when creating ADS made it possible to solve the problems of timely and reliable detection of deviations in LDS components. This is automates the detection of information threats and has led to an increase of information security in LDS and the effective work of system administrators and network security specialists.

REFERENCES

1 Barabanov A.V., Markov A. S., Tsirlov V. L. Certification of access detection systems // open systems. DBMS. 2012. -No. 3. - S. 31-33.

2 Girik A.V. Zhigulin G. P. Principles of formation the profile of the normal functioning of monitoring objects in the tasks of detecting network anomalies / / Journal "SPIIRAN works". - 2013. - pp. 172-181.

3 Michael Collins. Network Security Through Data Analysis: Building Situational Awareness. - 2014. - P.20.

4 Chris Sanders. Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems. - 2017. - P.145.

5 Sherri Davidoff, Jonathan Ham, Network Forensics: Tracking Hackers through Cyberspace. - 2013. - P.65.

6 Stephen Northcutt, Judy Novak. Network Intrusion Detection. - 2013. - P.267.

7 Richard Bejtlich. The Tao of Network Security Monitoring: Beyond Intrusion Detection.- 2014. - P.75.

8 Gromov Yu.Yu., Drachev V. O., Ivanova O. G., Shakhov N. G. Information security and protection of information. - M.: LLC "TNT", 2010. - 384 p.

9 Babash A.V., Baranova E.K., Larin D. A. Information security. History of protection of information in Russia. - M.: ID KDU, 2013. - 736 p.

10 Lariontseva E. A., Markov A. S., Stelmashuk N. N. Multi-factorial models of planning certification of software sources of information protection // Issues of radio electronics. - 2013. - №2. - P. 76-83. (17.12.2023)

11 Cisco. The NetRanger Intrusion Detection System.URL: http://www.cisco.com/warp/public/778/security/netranger/netra_ds.htm.(16.12.2023)