Oleh HARASYMCHUK[1], Vasyl RAMSH[2], Viktoriia TYSHCHENKO[3]

Opiekun naukowy: Oleh HARASYMCHUK[1]

THE ANALYSIS OF THE METHODS OF COMPUTER INFORMATION SYSTEMS PROTECTION BY MISLEADING THE ATTACKER

Summary: Modern approaches to the protection of computer information systems were analyzed. Deceptive information systems were classified.

Keywords: computer information system, attacker, attack, deceptive information system, network, unauthorized access, host.

ANALIZA METOD OCHRONY KOMPUTEROWYCH SYSTEMÓW INFORMACYJNYCH PRZEZ WPROWADZENIE NARUSZYCIELI W BŁĄD

Streszczenie: Przeanalizowano nowoczesne podejścia do ochrony komputerowych systemów informatycznych. Zostały sklasyfikowane zwodnicze systemy informacyjne.

Słowa kluczowe: Komputerowy system informacyjny, atakujący, atak, wprowadzający w błąd system informacyjny, sieć, nieautoryzowany dostęp, host

1. Introduction

Despite the significant results of theoretical and applied research in the field of information security in computer information systems (CIS), in particular with applying cryptographic methods, reservation, methods of interconnectivity control,

[1] PhD, Lviv Polytechnic National University, Associated Professor of Information Protection Department, oleh.harasymchuk@gmail.com

[2] PhD, Separated Subdivision of National University of Life and Environmental Sciences of Ukraine Berezhany agrotechnical institute, Associated Professor of Energy and Automatics Department, ramsh_v@ukr.net

[3] Lviv Polytechnic National University, student of Information Protection Department, vikatishtshenko@gmail.com

etc., the problem of protection of CIS connected to public communication networks remains insufficiently processed.

Given that in many cases CIS objects are equipped with different types of computational tools, existing methods of providing information security with the help of "protective shells" are not always effective and can be easily exposed to destructive influences of the "denial of service" type. The main disadvantage of existing methods and measures for information security, including modern means of finding vulnerabilities in automated systems and detecting unauthorized actions, is that in most cases they organize information protection against detected threats only, which shows a degree of protection passivity.

One of the possible solutions to the problem of protecting the information in CIS against unauthorized actions is to use methods of deception. Such systems have been called erroneous or deceptive. The mechanism of functioning of the deceptive system is to involve the attacker in a dialogue with the system. In this case, deceptive systems mimic the vulnerabilities of real information systems. The attacker has to constantly decide whether he is working with the real system or the erroneous one while wasting resources. The user who follows all the instructions overcomes all the areas in the least amount of time.

1.1. Structural model of information threats in CIS

In general, the CIS includes many hardware, software and technical means that are interconnected by data transfer channels. These means are united into a coherent whole from a set of territorially dispersed elements.

At the lower level of detail, CIS can be represented as a set of hardware and physical connections between them. At the top level of detail, it can be represented as a set of application flows with the help of which substantial information processing is carried out, as well as the rules of information exchange in the interests of application flows interconnection.

Structural model of information threats in CIS is shown in Figure 1.

Modern CISs must include the following elements:

1. System users' workplaces from which simultaneous access of users from various categories and with various privileges to access to shared resources of CIS is carried out. Such workplaces are the most affordable component of CIS. From most of them unauthorized actions can be attempted.

2. CIS information resources (based on file servers, print servers, databases, WEB, etc.), which can be either separate or combined with particular workstations and are intended to implement functions of file and data storage, printing, workstation maintenance, and other actions.

3. Communication equipment, that connects multiple data transfer networks, or different segments of the same CIS. Servers and communication equipment as the most important elements of a CIS require special protection. This is because large volumes of information and software are concentrated on the servers and with the help of communication equipment the information is processed with the alignment of the protocols of exchange between different segments of the network. Considering the isolated location of these CIS elements and the limited number of people who have access to them, accidental influences of system users can be considered almost impossible. However, in this case, there is an increased risk of remote deliberate

destructive impacts execution on these elements of the system with the exploitation of errors in their configuration, shortcomings of protocols used, software weaknesses.
4. Software (operating systems, application software, etc.) is the most vulnerable component of CIS since in most cases various attacks on CIS are conducted using software vulnerabilities.
5. Communication channels (dial-up/dedicated, radio channels/wirelines, etc.) are of great length, so there is always a likelihood of unauthorized connection to them and, as a result, the reading of transmitted information or interference with the transfer process itself.

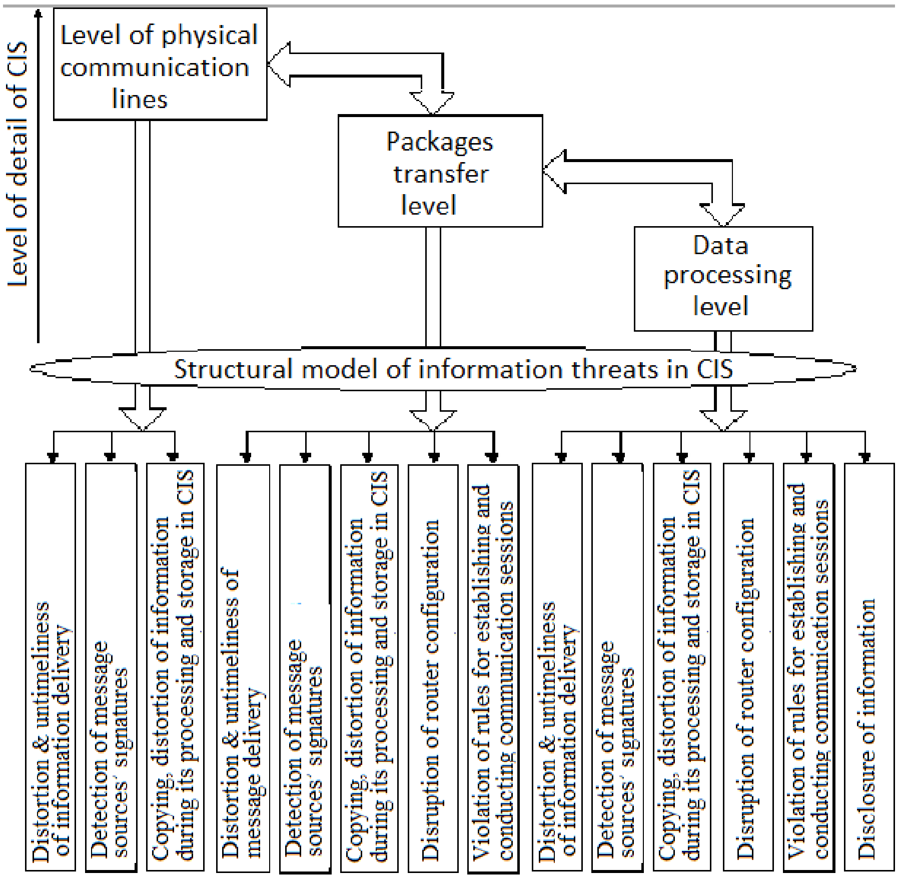
Level of detail of CIS
Level of physical communication lines
Packages transfer level
Data processing level
Structural model of information threats in CIS
Distortion & untimeliness of information delivery
Detection of message sources' signatures
Copying, distortion of information during its processing and storage in CIS
Distortion & untimeliness of message delivery
Detection of message sources' signatures
Copying, distortion of information during its processing and storage in CIS
Disruption of router configuration
Violation of rules for establishing and conducting communication sessions
Distortion & untimeliness of information delivery
Detection of message sources' signatures
Copying, distortion of information during its processing and storage in CIS
Disruption of router configuration
Violation of rules for establishing and conducting communication sessions
Disclosure of information

Figure 1. Structural model of information threats in CIS

1.2. Analysis of modern approaches to the protection of CIS

In general, the protection of CIS can be divided into two directions (Fig.2): protection of information that is directly processed and stored in CIS and protection of CIS elements.

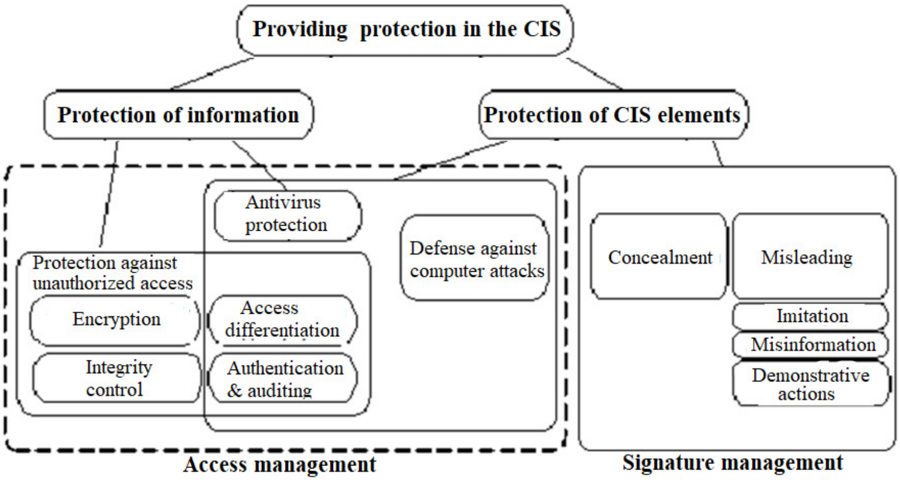
Providing protection in the CIS
Protection of information
Protection of CIS elements
Antivirus protection
Defense against computer attacks
Protection against unauthorized access
Encryption
Access differentiation
Integrity control
Authentication & auditing
Concealment
Misleading
Imitation
Misinformation
Demonstrative actions
Access management
Signature management

Figure 2. Analysis of modern approaches to the protection of CIS

1.3. History of the development of deceptive information systems (DIS) and the means of their creation

There are many different uses for deception in the purpose of protection. The most well-known among them are concealment, camouflage,misinformation.

In the area of information security, the first method concealment became the most widespread. An example of this method would be to hide the topology of a firewall-protected network segment.

An example of camouflage is the use of a Unix-like graphical interface on a Windows-based operating system, which causes an attacker who accidentally saw such an interface to attempt an attack that exploits a Unix OS vulnerability, and not Windows. This approach significantly increases the time it takes for an attacker to "successfully" launch an attack.

As an example of misinformation, we can consider the use of headers (banners), which allows the attacker to form a false idea about the system. The implementation of these methods of deception in practice is performed by deceptive information systems (DIS), also called deceptive systems.

Generally, the goal of a DIS is to emulate certain known vulnerabilities that do not exist in the protected system in reality.

1.4. DIS classification

The DIS serves to implement mechanisms for misleading the attacker in order to complicate and prevent attacks on target automated information systems (AIS) and to impose specially prepared false information. DIS is traditionally viewed as a security resource that is designed to investigate violent attacks. Thus, the indirect impact of DIS on enhancing the security of protected AIS is reflected in the disclosure of violators' strategies, methods and means of action to further strengthen defense mechanisms.

The direct impact of an DIS on the security of the AIS may be manifested in the strengthening of the overall security architecture and specific protection mechanisms by diverting attention of violators from the components of the target system which is protected by the components of the deceptive system and the implementation of more effective mechanisms for responding to the attacker's actions, as well as using firewalls, detecting attacks, etc.

Deceptive information systems can mimic a separate protocol (SMTP, FTP, SOCKS, HTTP, SSH, Telnet, etc.), a separate workstation or server running the operating system, and network goals, vulnerabilities, and security.

Deceptive information systems must be classified by four main features:

1. *By the level of integration of the DIS in the target AIS*(separated from the target AIS, parallel to the target AIS, part of the target AIS).

Those DISs that are separated from or parallel to the target AIS can be designed to distract forces and misinform attackers, gather information about them, study attack behaviors, detect and alert attacks.

DISs that are a part of the target AIS can be the most effective and complicate to set up and operating. They allow us to detect, track, stop attacks from the inside, and misinform attackers.

2. *By purpose* (production DIS, research DIS).

Production DISs are used to protect AIS resources and reduce the risk of their subversion. They are usually easier to implement because they have less functionality than research DISs. However, they may provide less information about the attacker.

Production DIS should promote the implementation of the three main functions of protection of the AIS from attacks: obstruction, detection, and reaction by connecting deceptive mechanisms based on the basic goals of the attacker to implement the threat of violation: confidentiality, access, integrity. Traditional security mechanisms to prevent attacks are firewalling, access control, authentication, and encryption.

If the attack is aimed at the implementation of the privacy threat, the DIS can imitate an object that contains specially prepared open and supposititious confidential information. (Fig. 3)

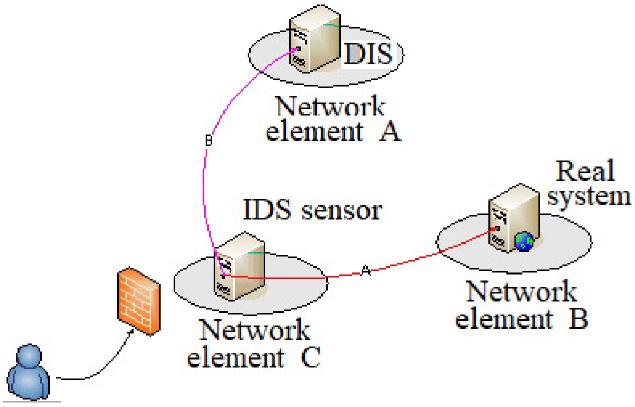

Figure 3. An example of simulating erroneous objects to misinform the attacker or to distract from the real system

DISs are directly involved in detecting attacks. Traditional intrusion detection systems have significant drawbacks: a large number of false positives and the inability to detect unknown attacks. DIS help to improve the number of false positives, the number of missed attacks, the ability to detect hidden and new attacks, and the aggregation of data. This is because the volume of traffic sent to the DIS (compared to the target AIS) is small and practically all this traffic is malicious.

Production DISs can be used to take action in response to an attack or to analyze the situation in the AIS that an attacker has penetrated. Deceptive information systems respond to an attacker's actions by misleading (deceiving) them and help to gather Research DISs are used to study the actions of an attacker, the strategies and tools they use to build more effective mechanisms for protecting and enhancing the security of the target AIS. DISs of this type are characterized by a high level of interaction with the attacker. They allow you to track the attacker's action of compromising the systems step-by-step, fix them, study attack methods, carry out pre-emptive warnings and predict attacks. They are more complex and use not simulated, but real operating systems and applications. However, higher functionality leads to higher maintenance costs and a greater risk of compromising and using them against other systems compared to production DISs.

The well-established term for the simplest DIS is the word honeypot. This term usually means a fake computer system installed as a "bait" used for research purposes. An example of an international research project is the Honeynet project, which aims at creating DISs around the world, investigating the behavior of malicious users with their help and detecting new malware and computer attacks.

In their development history, the DISs of the honeynet project can be divided into first and second generation.

First generation

The early DISs of the honeynet project consisted of several components:

– firewall - configured 'backwards' to block the attacker's traffic originating from the compromised honeypot to other hosts on the Internet;

– a honeypot host;

– sniffer - listens in stealth mode, without an IP address, capturing traffic without revealing itself to the attacker;

– log-host - capturing system logs from the honeypot.

The idea of such a system is to log an intruder's attack on the bait host. The hidden traffic analyzer logs all attempted attacks, but cannot be accessed because it does not have an IP address. The registration data on the hard drives of the bait host and the log-host is allowed to be deleted by the attacker. Precisely because such systems enable the attacker to perform the actions they want, these systems are classified as high-level DISs.

The attack is supposed to be reconstructed manually from the traffic analyzer log files. Strengthening the firewall policy is difficult because it should not block too much of the attacker's actions. Otherwise, it might display itself too early.

Second generation

The 2nd generation is an improvement of the 1st generation. They consist of:

– bridge that logs traffic at 2 levels of a reference model of open systems interaction;

– bait host (honeypot).

Virtual honeynet

Virtual machines (e.g. User-Mode Linux, VMware [1]) allow you to simulate honeynet by creating virtual hosts. They have several advantages. Such networks are easy to set up and the configuration can be easily restored. The host system can monitor the virtual machine. Virtualization technologies can be used to reduce the cost of hardware for DIS development.
However, there are several specific disadvantages:iingle point of failure and high requirements for the virtualization system.

Hybrid virtual honeynet

A hybrid virtual honeynet is a hybrid of classic honeynet and virtualization software. As in the sensors of attack detection systems, data interception, firewalling, and information analysis are conducted on a separate, isolated system. This isolation reduces the risk of hacking. However, all DIS nodes are implemented in a single system.

Dynamic DISs

Dynamic DISs are quite promising [2]. Such systems should passively generate false resources in the DIS by listening to the network when detecting the activity of the attacker according to his requests. The idea is that any deceptive resources, up to misinformation files, can be used as a bait.

Honeypot Farms

Honeypot Farms is a solution to the problem of deploying a large number of erroneous hosts in a DIS.The idea is to deploy a centralized honeypot farm (the modern term used to refer to a group of servers) consisting of several high- and low-interaction honeypots or even honeynets and then to deploy traffic relocators that redirect the traffic to the centralized honeypot farm (Fig. 4).

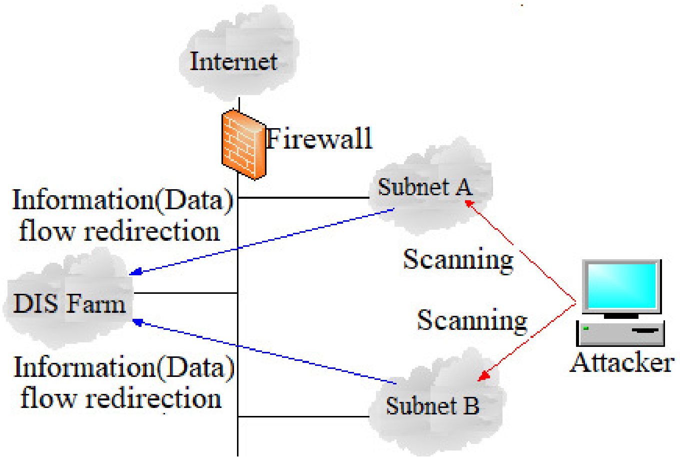

Figure 4. Honeypot Farm solution architecture

3. *By the level of misleading (deceiving) the attacker (Fig. 5):* segment level, host level, – service/application level.

At the segment level, the DIS simulates the target system. When an attack is detected, the attacker is redirected from the target AIS to the DIS.
At the host level, the DIS simulates the host of the target AIS (workstation, server) and is located on its network.

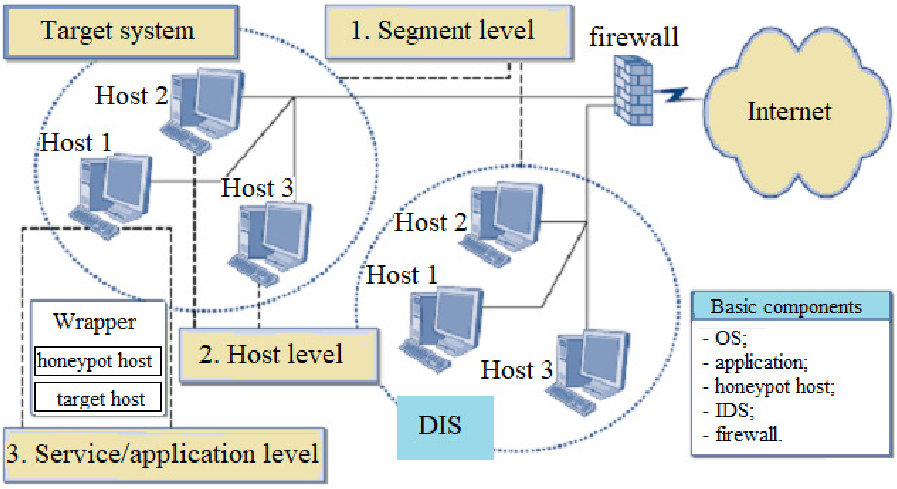

Figure 5. Generalized OIS architecture and misleading levels implementation

4. *By the level of interaction with the attacker:*

– low;
– medium;
– high.

The level of interaction with the intruders determines what opportunities the DIS provides to them in the implementation of the attacks. The more freedom an attacker has, the bigger the amount of information you can gather about his actions. Additionally, the higher the level of interactivity and the interaction time are, the greater an amount of work to install and maintain the system and the risk of compromising it would be.
Production DISs usually have low interaction level. They simulate services (and related OSs), limiting the number of actions that can be done to DIS by an attacker. This interaction is limited by how detailed the simulated services are. Unlike high-interaction DISs, there is no real OS that an attacker has access to. The advantage of low-interaction DISs is their ease of setting up and the significant reduction of the system compromise risk.
The primary purpose of low-interaction DISs is to detect attacks, including unauthorized scanning and connection attempts, as well as warnings of suspicious activity. OIS data allows you to collect the following attack information:
– time and date of the attack;
– address and port of the source of the attack;
– address and port of the destination of the attack, etc..

If emulated services interact with the attacker, the DIS can capture the actions of the attacker. The completeness of the tracking of the attacker's actions depends on the DIS emulation capabilities. The disadvantage of such DISs is that they cannot track and collect more detailed information (such as IRC chats, e-mail, etc.).

Medium-interaction DISs have more advanced interaction capabilities than low-interaction DISs. However, they have less functionality than high-interaction DISs.

A distinctive feature of such DISs is the creation of virtual OS instead of service simulation implementation. The virtual OS is controlled by the real OS and provides specifically limited functionality of the real OS to reduce the risk of system compromise. The high functionality of these DISs allows simulating the work of network segments, servers, workstations, including their vulnerabilities for lure and deception.

Medium-interaction DISs allow to effectively detect, secretly track, restrain and quickly analyze attacks. They detect intrusions into hosts and networks while reducing costs by minimizing the number of false positives and responding to attackers by incorporating deceptive mechanisms.

DISs with a high level of interaction are based on the use of real information resources, including operating systems and applications that use real services instead of simulated (HTTP, FTP, Telnet, etc.). Compared to low- and medium-interaction DISs, these DISs have significantly greater ability to capture attack information, however, they have a higher risk of compromise and usage for subsequent attacks. Such OICs are usually of the research type, although they can also be used as production ones. In order to reduce the risk of compromise and detection by the attacker, additional technologies such as firewalls and attack detection systems (ADS) should be used. A high-interaction DIS is a real computer system that differs from the target system in that it does not perform targeted tasks (does not contain real information) but serves to lure the attacker, to allow to secretly study their actions, and also to work out effective ways to automatically respond to attacks with attacker deception.

1.5. Analysis of known software DISs

To date, there are many software implementations of DIS elements of varying complexity, which include software products such as Deception ToolKit, Fakebo, Iptrap, Honeyd, KFSensor, and others.

1.6. Variants of modern DISs application

There are many options for using DIS to directly or indirectly enhance the security of protected resources:

1. *Improving the DIS security*

In networks where the internal security of the technical side leaves much to be desired, for the prevention of possible network incidents, usage of DIS (artificial network, honeynet) will allow [3]:

– identify the hosts from which the network is scanned;

– identify the hosts from which the IP packets are sent to non-existent network resources;

– identify the hosts from which attempts or prerequisites for the DOS attacks are made;

– identify the hosts from which the type of brute-force attack occurs (password selection by the brute force method);
– identify the hosts from which unauthorized attempts to send letters are made;
– identify the hosts from which unauthorized access to network resources is established;
– identify the hosts from which the targeted attack on network resources occurs.

2. *The fight against spam*

In practice, this possibility was used in the study described in [4]. This study uses the well-known Honeyd OIS deployment software tool. It is used to monitor spam mail relays opened by spammers. Networks with open mail relays and proxies were created. These networks intercept all spam-related emails and then analyze the reasons for receiving the spam. The captured email is sent to a shared spam filter that allows other users to avoid reading already known spam.

3. *DISs in the wireless networks*

The study described in [5] focuses on the detection of wireless attacks (attacks that involve the organization of unauthorized access to a secure wireless network based on the IEEE 802.11 standards). This research is part of one of the areas of activity of the Spanish branch of the honeynet project.
The described wireless DIS is called HoneySpot.

4. *Catching malware*

Probably the most widespread use of DIS is for catching new malware.
Microsoft has launched the Strider Honeymonkey Exploit Detection System (SHEDS) project. It is an automatic search engine for sites that distribute programs with potentially dangerous consequences, such as trojans or exploits. The difference between SHEDS and the Honeynet project is as follows. The passive Honeynet network works as a bait - passively awaiting infection. The hosts of the "active" SHEDS network "look for trouble" themselves. These sites automatically browse the "questionable" resources of the Internet trying to find sites that infect computers.
The main idea behind the project was to introduce the new exploit, Trojan, and spyware programs before they became a reality.

5. *DISs in SCADA system*

Also known are the studies aimed at creating an DIS for industrial control systems (SCADA systems). The purpose of the project is to gather information about the vulnerabilities and weaknesses of the architecture of modern SCADA systems from a security perspective. Work is under way to create tools that can simulate client-server ICSs, distributed ICSs, and programmable logic controllers (PLCs). Cisco Systems, Inc. specialists are working on the project.

2. Conclusions

From the above analysis, we can conclude that the direction of protection of information of the protected object in modern CISs is practically not implemented.

Only the task of blocking unauthorized access to the processed information and elements of CIS is solved.

At the same time, an analysis of the capabilities of existing DISs shows that they could take on the function of preventing attacks on CIS elements, thereby significantly enhancing their security. However, to date, DISs are usually assigned the role of lures, which are used to explore the possibilities of attackers and to analyze their actions.

Therefore, the results of the analysis of the conditions of functioning of modern CISs and DISs, conducted above, made it possible to formulate the following task: the development of effective methods and algorithms for the functioning of deceptive information systems is required**.**

REFERENCES:

1. Inc. VMware workstation: *http://www.vmware.com/support/,* 14.10.2019.
2. SPITZNER L.: Honeypots: Tracking Hackers, Publisher: Addison Wesley, 2002. - 480 p.
3. EVTEEV D.: Deployment of the honeynet on FreeBSD: *http://www.securitylab.ru/contest/266417.php*, 14.10.2019.
4. Research: Honeypots Against Spam: *http://www.honeyd.org/spam.php*. 14.10.2019.
5. The Wireless Honeypot. Monitoring the Attacker's Activities in Wireless Networks. A design and architectural overview: *http://honeynet.org.es/papers/honeyspot/HoneySpot_20071217.pdf*, 14.10.2019.