Saimaa University of Applied Sciences

Technology, Lappeenranta

Mechanical Engineering and Production Technology

Alexander Strelchenko

SAFETY OF THE COMPUTER NETWORK

Bachelor’s Thesis 2010

ABSTRACT

Alexander Strelchenko
Safety of the computer network, 59 pages, 0 appendices
Saimaa University of Applied Sciences, Lappeenranta
Technology
Mechanical Engineering and Production Technology
Bachelor’s Thesis, 2010,
Tutor: Mr. Jukka Nisonen, Saimaa University of Applied Sciences
Key words: network system, safety, virus, protection.

The purpose of the work was to develop recommendations, and guide of actions to support the necessary safety level of a computer network.
The tasks were:
- The analysis of the literature and informational sources devoted to network security;
- The analysis of resources and methods of protection of computer networks;
- To develop the complex of necessary measures and resources for support of necessary level of safety of a computer network.

CONTENT

INTRODUCTION

In our days information is very valuable and important**,** like every other value, people try to save it from extraneous hands and eyes, especially valuable government classified information and private commercial information. In business the diligent competition assumes the rivalry based on observance of the legislation and conventional norms of morals. However, it is not a secret that some businessmen are trying by means of illegal operations to receive the information to the detriment of interests of other side and to use it for advantage in the market.

There are a lot of reasons of the activity of computer crimes and financial losses linked to them, essentially they are because of:

- Transition from traditional "paper" technology of storage and transmission of data to electronic and poor development of protection technology;
- Association of computing systems, creation of wide-area networks and the external access extension to informational resources;
- Increasing the complexity of the software.

Therefore, the main tendency characterizing development of a modern information technology is the growth of number of computer crimes and the plunders of confidential and other information linked to them.

In process of development of electronic payments technology, electronic documentation and other business systems, serious failure of corporate networks can simply paralyze operation of the whole corporations and banks that will lead to notable material losses.

It is obvious that data protection in computer networks throughout development of information systems has got on the first place on importance at the organization of computer networks, and as to operation with them.

At present there are three basic principles of informational safety which should provide:

- Data integrity (solution of a problem of protection against the failures which are carrying on to lose or change the information);
- Confidentiality of the information (solution of a problem of not authorized access to the information);
- Availability of the information to all authorized users (solution of a problem of failure in service).

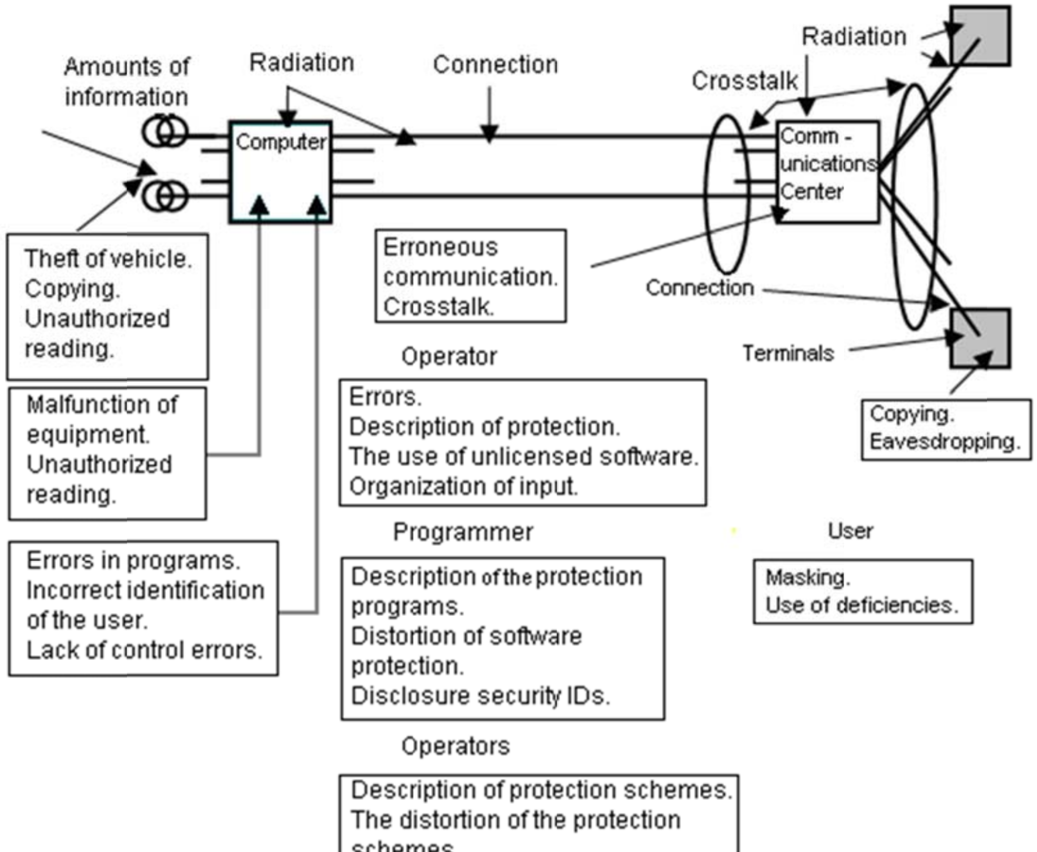
This work considers operation questions of protection of the information in computer networks. First the common safety issues of computer networks are considered, the main sources of threats are parsed. The second chapter is devoted to the analysis of the main methods and resources of support of informational safety. On the basis of the techniques considered in the second chapter, the third chapter analyses the support of informational safety of a company “Npp Inteps”. Because any company’s information that is stored and handled within the limits of a local area network represents a trade secret, questions of their protection are extremely important and actual for administration.

1. PROBLEMS OF SAFETY OF COMPUTER NETWORKS

1.1. Ways and methods of unauthorized access to information resources of computer networks

One of the major aspects of a problem of safety of computer networks is definition, the analysis and classification of possible threats of safety of the computer networks. The list of significant threats, estimations of probabilities of their implementation, and also the model of the infringer form a basis for carrying out the analysis of risks and a formulation of requirements to system are sewn up computer networks. The majority of modern informational networks of information processing generally represents territorially distributed intensively co-operating systems among themselves with given data (resources) and handler (events) of local area networks and separate computers.

Ways of unauthorized access to the information are resulted in figure 1.1 (Meshcherjakov V. A.. 2006, pp. 77-79)



Amounts of information
Radiation
Connection
Radiation
Crosstalk
Computer
Comm - unications Center
Theft of vehicle. Copying. Unauthorized reading.
Erroneous communication. Crosstalk.
Connection
Terminals
Malfunction of equipment. Unauthorized reading.
Operator
Errors. Description of protection. The use of unlicensed software. Organization of input.
Copying. Eavesdropping.
Errors in programs. Incorrect identification of the user. Lack of control errors.
Programmer
Description of the protection programs. Distortion of software protection. Disclosure security IDs.
User
Masking. Use of deficiencies.
Operators
Description of protection schemes. The distortion of the protection schemes. Wireless reading of information. Erroneous switching.

Fig 1.1 - Unauthorized access paths to the information.

All ways of "traditional" unauthorized access for locally allocated (centralized) computing systems in their operation and access to the information are possible. Besides, there are new specific methods of penetration into system and unauthorized access to the information.

Here is the list of the main features of the allocated computer systems (Devyanin P. N. 2005, pp. 24-27):

- Territorial separation of components of an allocated system and the intensive information exchange between them;
- Wide range of possible ways of representation, storage and information transfer protocols;
- Integration of the data of different function belonging to the various subjects, within the limits of uniform databases or vice versa, allocation of the necessary data in various remote networks;
- Abstraction of owners of the data from physical structures and a location of the data;
- Usage of methods of the distributed data processing;
- Usage of automated information processing systems of the large amount of users and staff of various categories;
- Direct and simultaneous access to resources (including valuable information) a great number of users of various categories;
- Varity of different hardware and software;
- Absence of special protection utilities that could be used in specific computer network.

Generally computer network system consists of the following main functional units (Devyanin P. N. 2005, pp. 32-34):

- Workstations - separate PCs or network terminals; where the users' automated work environment are realized;
- Host servers (file, databases, print and etc. services) - the high performance computers intended for implementation of functions of storage of the data, access and other operations;
- The network devices providing connection of several data networks;
- Data lines (local, broadband, etc.).

Modeling of processes of violation of informational safety is expedient to make that kind of a logical chain: «threat – a threat source – an implementation method – vulnerability – consequences» (Fig. 1.2.) (Hofman 2005, p.105)

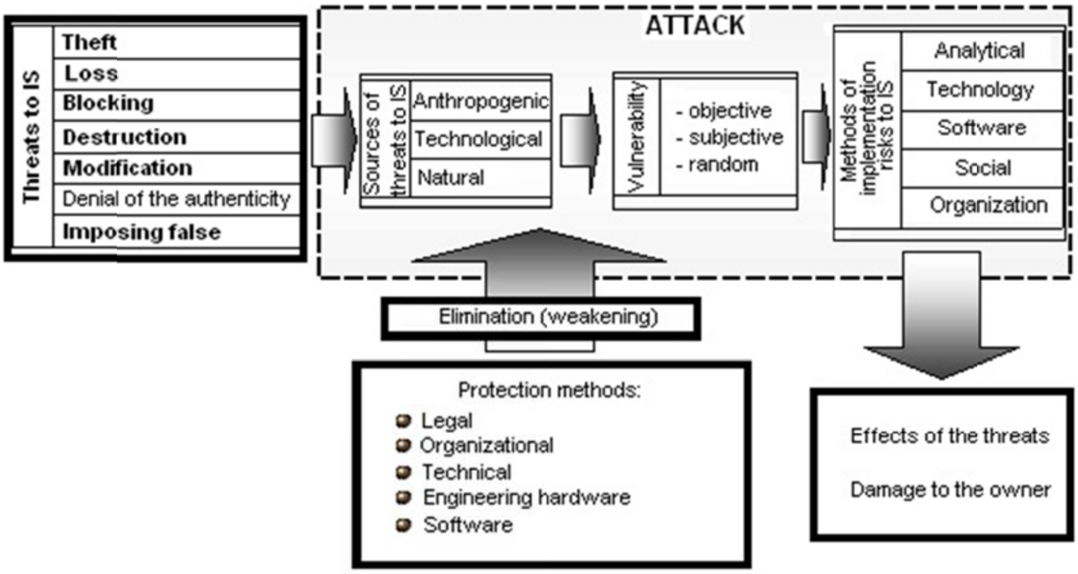


Fig. 1.2. Model of implementation of threats of informational safety

Unauthorized access to the information in a computer network happens:

1. Indirect - without physical access to units of a network and
2. Direct - with physical access to network units.

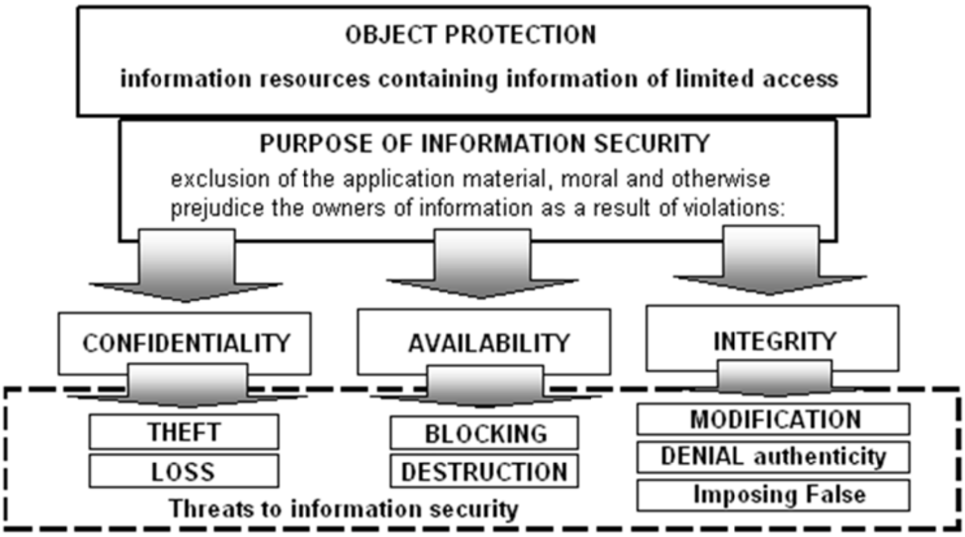

OBJECT PROTECTION
information resources containing information of limited access
PURPOSE OF INFORMATION SECURITY
exclusion of the application material, moral and otherwise prejudice the owners of information as a result of violations:
CONFIDENTIALITY
AVAILABILITY
INTEGRITY
THEFT
LOSS
BLOCKING
DESTRUCTION
MODIFICATION
DENIAL authenticity
Imposing False
Threats to information security

Fig. 1.3. The Purposes and threats of safety of the information [20, p. 117]

All sources of threats can be divided into the classes caused by the type of the carrier, classes share on groups on location (Fig. 1.4.).

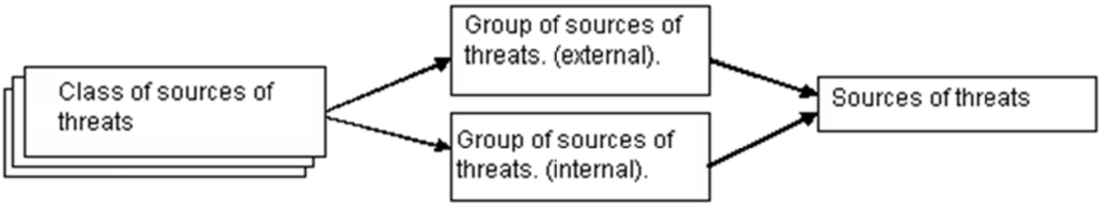

Class of sources of threats
Group of sources of threats. (external).
Group of sources of threats. (internal).
Sources of threats

Fig. 1.4. Classification structure «Sources of threats»

Classification of possibilities of a threat implementation represents a collection of various operations of a source of threats by certain methods of implementation with using vulnerabilities that lead to the realization of the attack.

1.2. The main sources of safety threats of computer networks

According to Domarev the main sources of threats of computer networks and information are:

- Natural disasters and accidents (flooding, hurricane, earthquake, a fire, etc.);
- Failures and refusals of the equipment (technical facilities);
- Development errors of computer networks components (hardware, technology of information processing, programs, data structures, etc.);
- Operation errors (users, operators and other staff);
- Deliberate operations of infringers (the offended persons from among staff, criminals, spies, saboteurs, etc.).

All kind of potential threats are divided into two classes by the nature of their occurrence: natural (objective) and artificial (subjective).

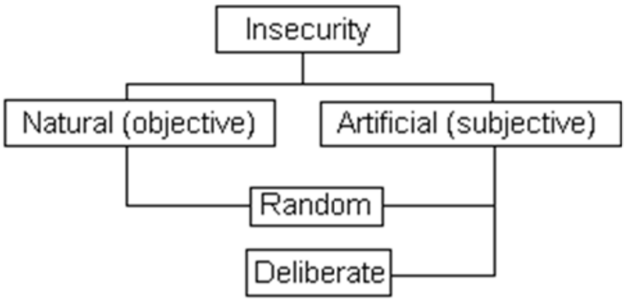


Fig. 1.5; Classification of threats by sources and to motivation (Shankin G.P. 2007, p. 117)

Natural threats are the threats called by effects on computer's network of objective physical processes or the spontaneous natural phenomena or disasters, independent of the human.

Artificial threats are called by activity of the person. Proceeding from motivation of operations among them, it is possible to select:

- Unintentional, casual threats called by errors in network designing, errors in the software, personnel errors, etc;
- Deliberate (premeditated) threats called by mercenary, ideological or other aspirations of people (intruder).

In relation to computer network, sources of threats can be external or internal (components of the networks by themselves - equipment, programs, staff, end-users).

The most common artificial threats of computer networks are (the operations made by people accidentally, on ignorance, carelessness or incompetence, but without malicious intention) (Gundar K.U. 2005, pp. 71-76):

1) The unintentional operations that lead to partial system crash or corruption of hardware, program, informational system resources;

2) Unsafe disconnecting of the equipment or change of operating mode of devices and programs;

3) Unintentional damage of information source;

4) The system software which is capable at incompetent usage to call system failure or carrying out irreversible changes in system;

5) Illegal implantation and usage of off-the-books programs with subsequent unreasonable expending of resources;

6) Infection of the computer with viruses;

7) The careless operations leading to share and disclosure of the confidential information;

8) Disclosure, transmission or loss of access information (passwords, encryption keys, identification cards, digital certificates, etc.);

9) Development of the architecture of the system, development of data processing technology, development of applications, with the possibilities of danger to the system and safety of the information;

10) Ignorance of company's limitations (corporate rules);

11) Logon bypassing protection bridges (loading of the extraneous operating system from replaceable storage devices, etc.);

12) Incompetent usage, customization or disconnecting of protection system by security staff;

13) Transfer of the data to the incorrect address (device, customer, etc);

14) Incorrect dada input;

15) Unintentional damage of data channels.

Based on Gundar's (2006, pp. 82-86) researches the main possible paths of deliberate disorganization, making system out of operation, penetrations into system and unauthorized access to the information are:

1) Physical corrupting (damage, frying, etc.) of the most important components of the computer system (devices, carriers of the important system information, etc.);

2) Disconnecting or frying of operation subsystems (power supplies, cooling and cooling, communication circuits, etc.);

3) Disorganization of system's functioning (change of operating modes of devices or programs, strike, staff sabotage, setting of a powerful active radio noise on frequencies of devices operation, etc.);

4) Implantation of agents as employees (including the management group which is responsible for security);

5) Recruitment (by payoff, blackmail, etc.) staff or the single users having certain powers;

6) Taps, remote a photo- and video-shooting, etc.

7) Interception of side electromagnetic, acoustic and other devices' radiation and communication lines, as well as pickups active radiation on support items that are not directly involved in processing information (phone lines, power supply, heating, etc.);

8) Interception of the data transferred by data channels. Further analysis for the purpose of finding-out the protocols of a data exchange, authorization rules in channel for subsequent penetration into system;

9) Plunder of data storage devices (magnetic disks, tapes, memory chips, storage devices and whole computer);

10) Unauthorized copying of storage devices;

11) Theft of industrial scrap (listings, the records, disposed documents, etc.);

12) Accessing to the remainder information from the RAM and from external storage devices;

13) Reading of the information from the RAM used by the operating system (including a security subsystem) or other users, in an asynchronous mode using disadvantages of the multitask operating systems and programming systems;

14) Illegal acquisition of passwords and other access information with the subsequent masking under the registered user;

15) Unapproved usage of users’ terminals having unique physical characteristics, such as workstation number in networks, the physical address, the address in a communication system, etc.;

16) Disclosure of crypt algorithm for crypted information or its codes;

17) Deployment of “specific software” and "viruses" ("trojans" and **"backdoors"),** allowing to brake security system, illegally and silently provide access to system resources for the purpose of recording and transmission of the confidential information;

18) Unauthorized connection to communication circuits for the purpose of operation "between the lines", using the pauses in operations of the real user from his name with the subsequent input of untrue reports or modification of transferred messages;

19) Unauthorized connection to communication circuits for the direct substitution of the real user by its physical disconnecting after logon and successful authentication with the input of misinformation and imposing of untrue reports.

Table 1.1; Classification of violation variations of working capacity of systems and unauthorized access to the information on objects of effect and ways of plotting of a damage of safety

Ways of plotting of a damage	Objects of effects			
	The equipment	Programs	Data	Staff
Disclosure (leak) of the information	Plunder of media, connection to the communication circuit, unapproved usage of resources	Unapproved copying interception	Plunder, copying, interception	Transmission of data on protection, disclosure, negligence
Information integrity	Connection,	Implantation	Distortion,	Staff

loss.	modification, activeX applications, change of operating modes, unapproved usage of resources	of Trojans and bugs	modification	recruitment, "masquerade"
Violation of working capacity of the automated system	Change of modes of functioning, output out of operation, plunder, corrupting	Distortion, removal, substitution	Distortion, removal, imposing of the false data	Maintenance, physical elimination
Illegal duplicating of the information	Manufacture of clones without licenses	Usage of illegal copies	The publication without the knowledge of authors	

The generalized classification of remote attacks:

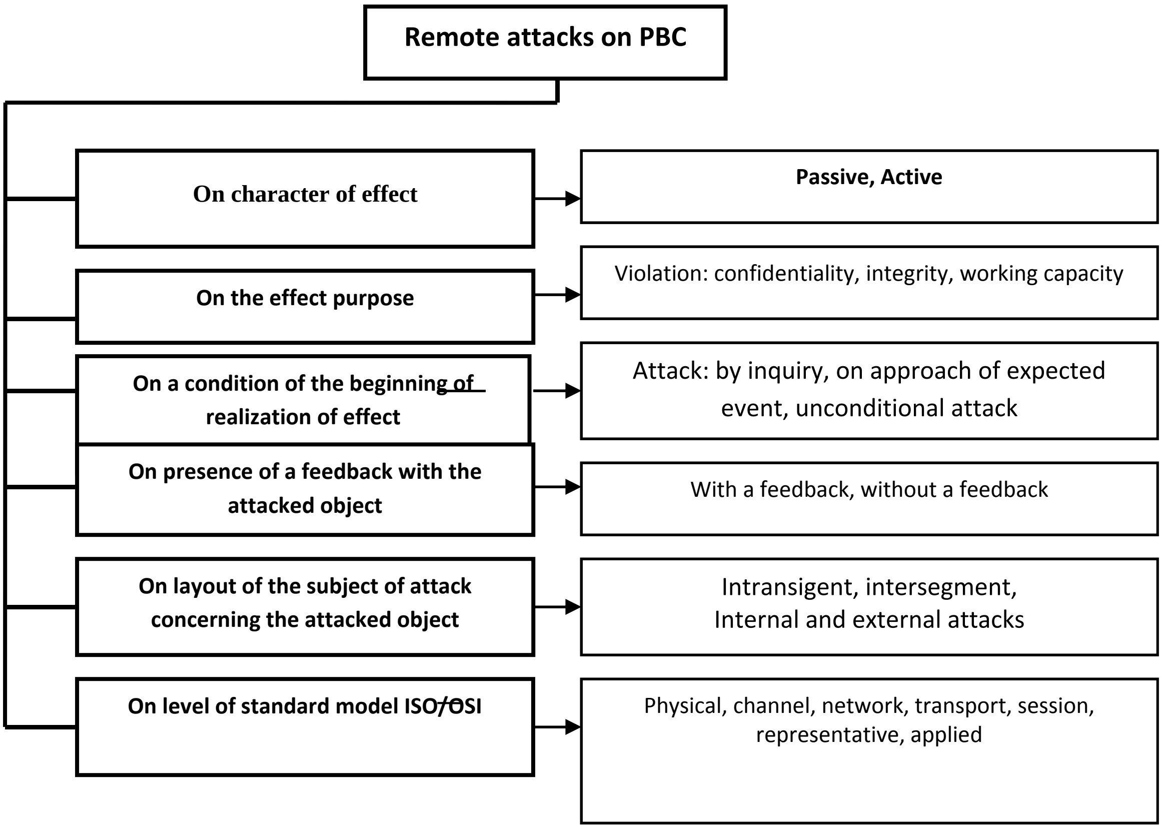

Remote attacks on PBC
On character of effect
Passive, Active
On the effect purpose
Violation: confidentiality, integrity, working capacity
On a condition of the beginning of realization of effect
Attack: by inquiry, on approach of expected event, unconditional attack
On presence of a feedback with the attacked object
With a feedback, without a feedback
On layout of the subject of attack concerning the attacked object
Intransigent, intersegment, Internal and external attacks
On level of standard model ISO/OSI
Physical, channel, network, transport, session, representative, applied

Fig. 1.6; Classification of standard remote attacks. (Gundar K.U. 2005, p. 96)

1.3. The characteristic and mechanisms of implementation of the standard remote attacks

The corporate network can be isolated from an external world (that is very conditional), or can have connection with the Internet. The typical configuration of a corporate network is presented in Fig. 1.7.

Being connected to networks of the common using, the organizations pursuit specific purposes and try to solve effectively the following tasks:

- To provide to internal users access to external resources. It is, first of all, WWW - resources, FTP - archives, etc;

- To give access to users from an external network to some internal resources (corporate WEB server, FTP server, etc.);

- To provide interaction with remote branches and offices;

- To organize the easy access to an internal network resources from any place.

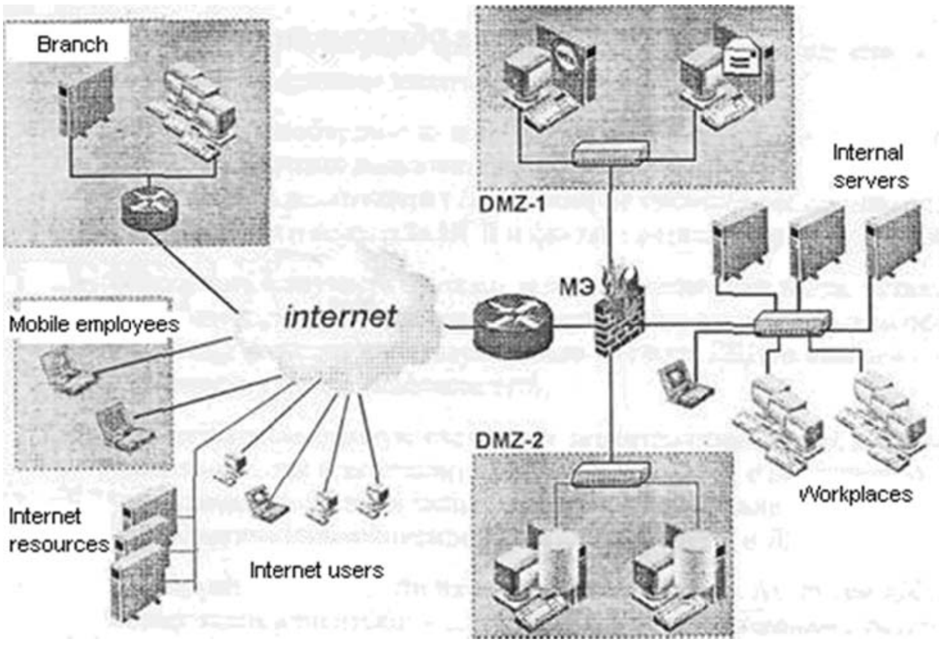


Fig. 1.7. A typical network configuration of the organization

Solving the enumerated tasks, the organization faces several safety problems. Interaction with remote branches and mobile users through open channels would create a threat of interception of the transferred information. Allocation of general access to internal resources creates threat of the external intrusions and receptions of the confidential information.

Having selected some levels of an informational infrastructure, it is convenient to consider about safety questions of corporate networks:

- Staff level
- Level of applications
- DBMS level
- OS level
- Network level

Network protocols concern network level (TCP/IP, NetBEUI, IPX/SPX), each has its own features, vulnerability and the possible attacks linked to them. Operating systems (Windows, UNIX, etc.) installed on nodes of a corporate network refers to operating systems (OS) level. It is necessary to select also level of database management systems (DBMS), since it is an integral part of any corporate network. At the fourth level there are the any possible applications used in a corporate network. It can be software Web servers, various office applications, browsers, etc. And, at last, on a top level of an informational infrastructure there are users and serving staff of the automated system.

It is possible to select some common stages of carrying out an attack to a corporate network: (Grinberg A.S.):

- Collection of data
- Attempt of gaining access to the least protected node (possibly, with the minimum privileges)
- Attempt of rise of privilege level or usage of nodes as a platform for research of other network nodes
- Complete control reception over one or several nodes

Intruder pursues specific purposes making those attacks. Generally they can be (Galatenko V.V., 2008):

- Violation of normal functioning of the attacked object (denial of service, DoS)
- Control reception over the attacked object
- Reception of the confidential information
- Modification and falsification of the data

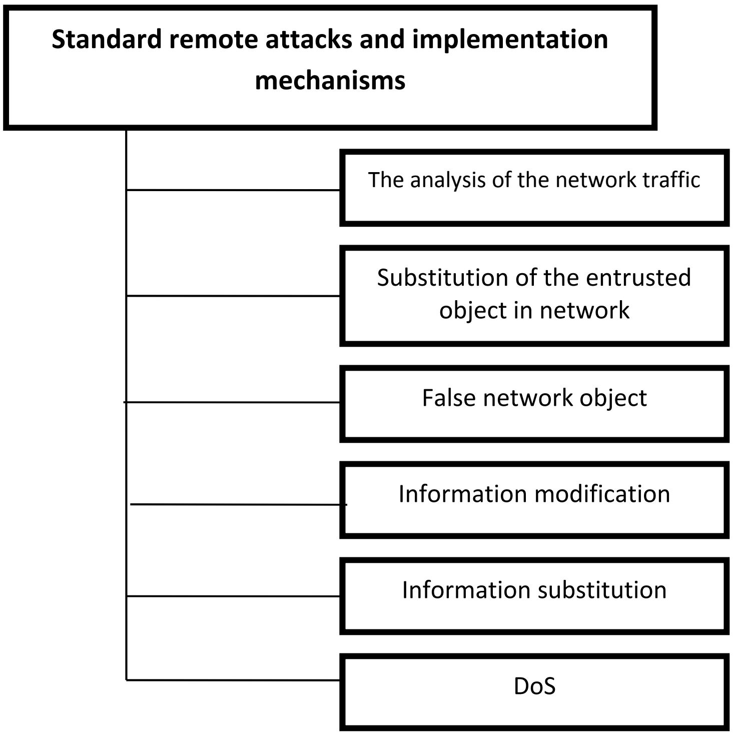

Standard remote attacks and implementation mechanisms
The analysis of the network traffic
Substitution of the entrusted object in network
False network object
Information modification
Information substitution
DoS

Fig. 1.8. Classification of standard remote attacks on distributed network systems

(Levin A.N. 2008, p.88)

The next possible variant of attack classification by location of the outrider:

- In one segment with the attack object;
- In different segments with the attack object.

The mechanism of implementation of attack depends on a relative positioning attacking and a victim. Usually implementation of intersegment attack is more difficult.

Most important for understanding the possible attacks is classifying the attacks by mechanisms of their implementation:

- Passive listening

Example: interception of the network traffic

- Suspicious activity
Example: scanning of ports (services) of the object of attack, attempt of password selection (bruteforcing)

- Useless expending of a computing resource

Example: exhaustion of resources of the attacked node or group of the nodes, leading to degradation (overflow connection requests, etc.)

- Navigation violation (creation of false objects and paths)
Example: Change of the path of network packages, so that they passed through hosts and routers of the infringer, change of corresponding maps of the conditional Internet names and IP addresses (DNS attack), etc.

- Disability
Example: transferring packages of certain type on the attacked node, leading to refusal of nodes or the services on it (WinNuke, applications for DoS attacks, etc.)

- Lunching applications on the attacked object
Example: execution of the hostile program in the RAM of the object of attack (trojans, control transfer to the hostile program by buffer overflow, fulfillment of a harmful code on Java or ActiveX, etc.)

The most complete classification of attacks is done by mechanisms of their implementation. Further examples of some mechanisms usage are (Galatenko V.V. 2007):

1) Traffic sniffing - interception and analysis of the network's traffic based on possibility of translation of the network adapter in nonselective operating mode.

The purpose: Reception of the confidential and critical information
The implementation mechanism: Passive sniffing
Used vulnerability: Based on the common environment of transmission technology (Ethernet)

- Disadvantage of designing, transferring of confidential information without encryption.

Level of an informational infrastructure: network.
Risk level: high.

2) Port scans - Connect to the network node and search in the selected range of ports to identify working services.

The purpose: reception of the confidential and critical information

Used vulnerability: service errors, installed but unused services.
Level of information infrastructure: network.

Risk level: low.

3) ARP Attack – Spoofing - Addition of false records in the table used by operation of ARP protocol

The purpose: Violation of normal functioning of the target of attack
The implementation mechanism: navigation violation
Used vulnerability: disadvantage of designing of ARP protocol
Level of an informational infrastructure: the network

Risk level: High

IISDOS Attack - Sending of incorrectly constructed HTTP-inquiry leads to the over-expenditure of WWW-server resources.

The purpose: Violation of normal functioning of the target of attack.

The implementation mechanism: useless expending of a server's resources. Used vulnerability: error of Microsoft Internet Information Server implementation.

Level of an informational infrastructure: Applications.

Rrisk level: Average

1.4. Information leak channels at physical level

The leak channel (LC) of information is a collection of a source of the information, the material carrier or the environment of distribution of a signal carrying this information and an assets of retrieving the information from a signal or the carrier. The following LC is known (Fig. 1.9)(Galatenko V.V. 2009):

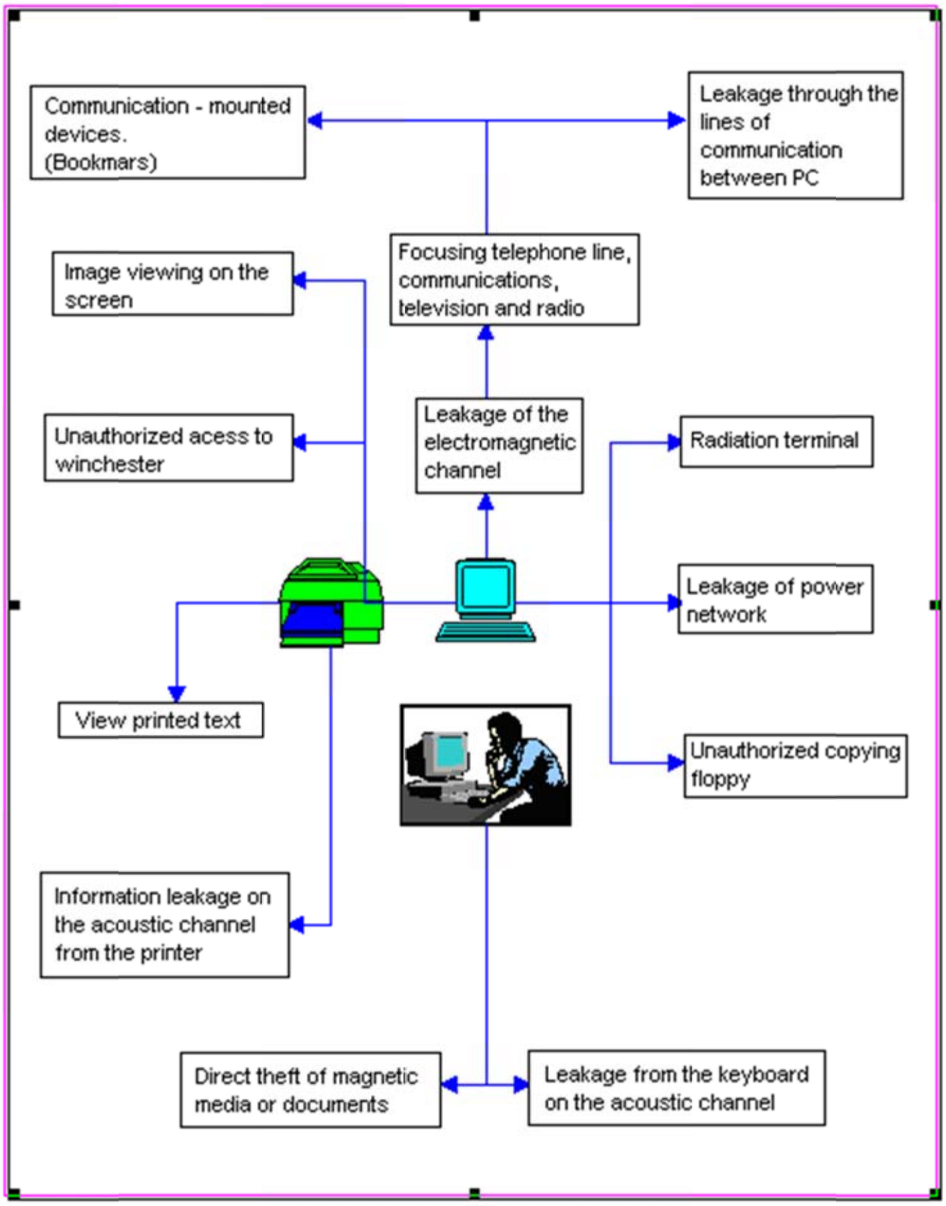

Communication - mounted devices. (Bookmars)
Leakage through the lines of communication between PC
Image viewing on the screen
Focusing telephone line, communications, television and radio
Unauthorized acess to winchester
Leakage of the electromagnetic channel
Radiation terminal
Leakage of power network
View printed text
Unauthorized copying floppy
Information leakage on the acoustic channel from the printer
Direct theft of magnetic media or documents
Leakage from the keyboard on the acoustic channel

Fig. 1.9. The main channels of information leakage while processing on the computer.

1. The electromagnetic channel. The reason of its occurrence is the electromagnetic field linked to electric current in devices while information processing. The electromagnetic field can induce currents in close allocated wires. The electromagnetic channel can be:

1.1. Radio channel (high-frequency radiations).
1.2. The low-frequency channel.
1.3. The network channel.
1.4. The grounding channel.
1.5. The linear channel (communication circuit between the PC).

2. The acoustic channel. It is linked to distribution of sound waves to air or elastic oscillations in other environments arising by operation of display units.
3. The unapproved copying channel.
4. The unauthorized access channel.

1.5. Viruses and harmful programs

1.5.1. Concept and types of computer viruses

Computer viruses are programs or fragments of a program code while having got on the target’s computer, can execute against will of the user various operations on this computer - to create or delete objects, to update datafiles or program files, to carry out operations in own distribution through local area networks or in Internet. Modification of program files, datafiles or boot sectors of disks in such a manner that they become carriers of a virus code by themselves, is named infection and it is the major function of computer viruses.

Depending on types of infected objects various types of computer viruses are exist (Bezrukov N.N. 2007, p. 33):

- Polymorphic viruses
- MtE computer viruses (Mutation Engine viruses)
- Memory resident virus
- Script virus
- Stealth virus
- Encrypted viruses
- Anti-antivirus Virus, Retrovirus
- Antivirus Virus

- Worm-virus
- The virus mystifier (Hoax)
- Virus-companion
- Dropper
- Zoo virus

Depending on sorts of infected objects, computer viruses can be divided into following types:

- File computer viruses (File viruses),
- Load computer viruses (Boot viruses),
- Macrocommand computer viruses (Macroviruses).

1.5.2. Classification of computer harmful programs

According to Bezrukov(2007, pp. 61-66) anti-virus laboratories classify the computer harmful programs using different algorithms of operation:

- Zombies — the small computer programs distributed in Internet by worm viruses. Zombie programs install themselves in the attacked system and wait for further commands to operation.

- Keyboard interceptors (Keyloggers) — sort of trojan programs, the main function of which is interception of the data entered by the user through the keyboard. The targets are personal and network passwords, the login information, credit cards and other personal information.

- Logic bombs — sort of Trojan program - the hidden units which have been built in earlier developed and widely used program. They are resources of computer sabotage. Such programs are harmless until a specific event when it exectutes (pressing by the user of certain keyboard buttons, changes in a file or approach of certain date or time).

- Backdoors — the programs providing logon or reception of exclusive rights bypassing existing security system. They are often used for detour of an existing safety system. Backdoors do not infect files, but register themselves in the register, updating register keys.

- Mail bombs — one of the elementary network attacks. The malefactor dispatches on the computer or a company mail server one huge message, or set of mail messages (ten thousand) that lead the system down.

- Rootkit — the harmful program intended for interception of system functions API operating system for the purpose of hiding the presence at system. Besides, rootkit can mask processes of other programs, various keys of the register, a folder, and files. Rootkit extends as independent programs and as additional components as a part of other harmful programs - backdoor, mail worms and other.

According to operation principle rootkits conditionally are divided into two groups: User Mode Rootkits (UMR) - rootkit, working in a user mode, and Kernel Mode Rootkit (KMR) - rootkit, working in a kernel mode. Operation UMR is based on interception of functions of libraries of a user's mode, and operation KMR is based on installation in system of the driver which execute interception of functions at level of a system kernel that considerably complicates its detection and neutralization.

- Trojans (Trojan Horses) — the harmful programs containing the hidden module, carrying out unapproved operation in the computer. These operations are always aimed at harming the user. Trojans substitute some often started programs, perform its functions or imitate such performance, simultaneously making some harmful operations. Some Trojan programs contain the mechanism of upgrading the components from the Internet.

- Applets - applications, small Java-applications which are built in HTML page. Inherently, these programs are not harmful, but can be used in the ill-intentioned purposes. Especially applets are dangerous to fans of on-line games since Java applets are used there. Applets can be used for sending the information gathered on the computer to the third party.

- Web bugs - a tracing resource for networkers the Internet. Usually transparent, graphics files with the size of 1x1 pixel used for collection of the user‘s statistical information when user is coming on a web site. These bugs can gather different kind of information - date and time, browser type, screen settings, JavaScript settings, cookie, the IP address, type of the operation system. Spamers use such bugs, including them in dispatched e-mails that give the chance to them to define existence of the address.

- Page interceptors (hijackers) - sort of the undesirable computer program the purpose of which to install necessary page as start page on the computer where trojan could get. Programs use security faults in Internet browsers and register themselves in the registry. Usually, hand cleaning of the register does not help; such trojans have function of restoring the necessary data in the register and disguise as system files.

- Cookies files - files which consist the data about the user, gathered by web servers and stored on a computer hard disk. While visiting any web server the special files, cookie, save information of the visitor which is used for identification of the user by the server. The data received from files cookie, is used by spamers for compilation of lists of dispatches.

- Spybots - not viruses, usually used by hackers for tracing network ability.

- Spyware – dangerous programs to the user (not viruses), intended for tracing behind system and sendings of the gathered information to the third party - to the creator or the customer of this program. Presence of the spyware software on the computer leads to astable operation of a browser and deceleration of the system.

2. PROTECTION METHODS OF COMPUTER NETWORKS

2.1. Threat model of the corporate computer network

Proceeding from the analysis, all sources of safety threats of the information appearing in a corporate network can be divided into three main groups (Jurasov J.V., Kulikov G. V 2005):

I. The threats caused by operations of the subject
II. The threats caused by hardware (technogenic threats)
III. The threats caused by spontaneous sources (natural disasters)

The perpetrators operations can lead to violation of safety of the information can be external:

1. Criminal structures;
2. Recidivists and potential criminals;
3. Unfair partners;
4. Competitors;
5. Political opponents;

As well as internal:

1. Company’s staff;
2. Branches’ staff;
3. Competitors’ agents.

Based on the results of the international experience, operations of perpetrators can lead to a number of undesirable consequences among which with reference to a corporate network, it is possible to mark out the following:

1. Theft of

- Hardware (hard disks, notebooks, system units);
- Data carrier (paper, magnetic, optical and etc);
- Information (reading and unapproved copying);
- Access information (keys, passwords, and etc);

2. Substitution (modification) of

- Operating systems;
- Database management systems;
- Applications;
- The information (data);
- Passwords and access rules;

3. Destruction (corrupting) of

- Hardware (hard disks, notebooks, system units);
- Information carriers (paper, magnetic, optical and so forth);
- The software (OS, a DBMS, operationing software)

- Information (files, data)
- Passwords and the key information.

4. Violation of stable operation (interruption) of

- Speeds of information processing;
- Capacity of data links;
- Sizes of the free RAM;
- Sizes of a free disk space;
- Power supplies of hardware;

5. Errors

- At software installation, OS, a DBMS;
- At a developing of software;
- At maintenance of hardware;

6. Interception of the information (unapproved)

- With specific hardware;
- By to interference from power lines;
- By to interference by outside conductors;
- By the acoustic channel from output media;
- By the audio channel at discussion of questions;
- By connection to information transfer channels;
- By violation of the rules of access (hacking);

The second group contains threats less predicted, directly depending on technical properties and consequently demanding special attention. The technical means, containing potential safety threats of the information as can be internal:

1. Poor-quality hardware of information processing;
2. Poor-quality software of information processing;
3. Auxiliary means (guarding systems, alarm systems);
4. Other means applied in offices;

And external:

1. Communication facilities;
2. Close allocated dangerous productions;
3. Service lines (energy and water supply, the water drain);
4. Transport.

Consequences of application of such means, directly influencing safety of the information can be:

1. Violation of operating stability

- Violation of workability of a data processing systems;
- Violation of workability of telecommunications;
- Ageing of media resources;
- Violation of the existent access rule;

2. Destruction (corrupting) of

- The software, OS, a DBMS;
- Information processing resources (power hit, leakings);
- Premises
- Information (demagnetization, radiation, leakings and etc);
- Staff

3. Modification of

- The software, OS, DBMS;
- Transmitted information through data links and communication links.

The third group is made by threats which are impossible to predict and consequently monitoring of their potential activity should always be applied. Unpredictable threats are usually considered as natural disasters, like:

1. Fires;
2. Earthquakes;
3. Flooding;
4. Hurricanes;
5. Various unpredicted circumstances;

6. The inexplicable phenomena.

These natural disasters and inexplicable phenomena as influence of the informational safety are dangerous to all units of a corporate network and can lead to destruction and loss of important information, hardware, staff members and etc.

2.2. The main mechanisms of protection of computer systems

For protection of computer systems against unauthorized interference in processes of their functioning and information the following main protector methods are used:

- Identification (naming and identification), authentication (authenticity confirmation) users of system;
- Access differentiation of users to system resources and authorization (assignment of rights) to users;
- Registration and notification about the events occurring in system;
- Cryptography of stored and transferred on data links;
- The integrity and authenticity control of the data;
- Revealing and neutralization of operations of computer viruses;
- Overwriting of the remainder information on data carriers;
- Identifying the vulnerabilities (weak places) of systems;
- Computer network isolation (traffic filtering, concealment of internal structure and addressing, etc.);
- Detection of attacks and operative reaction;
- Backup;
- Masking;

The listed mechanisms of protection can be applied in concrete means and protection systems in various combinations and variations. The greatest effect is reached at their continuous usage with other sorts of protection. We will consider the listed protective mechanisms in more detail.

2.2.1. Identification and authentication of users

With a possibility of access differentiation to resources of computer network and possibility of registration of each access (the employee, the user, process) and the resource of the protected automated system should be identified. For this purpose special tags of each subject and the object by which they could be identified should be stored in the system.

Identification is, on the one hand, assignment of individual names, numbers or special devices (identifiers) to subjects and system objects, and, on the other hand, is their identification by the unique identifiers assigned by it. Identifier presence allows simplifying procedure of selection of the concrete subject from set of the same subjects. Numbers or symbols in the form of a character set are applied more often as identifiers.

Authentication is a confirmation of authenticity of identification of the subject or system object. The purpose of authentication of the subject is to be convinced that the subject is who was identified. The purpose of object authentication is to be convinced that it is that object which is necessary.

According to Levin (2004, p. 129) usually the authentication of users is carried out:

- By checking the knowledge of passwords by them (special confidential character strings);

- By checking their possession of any special devices (cards, keys, etc.) with unique tags;

- By checking unique physical characteristics and parameters (i.e fingerprints, etc.) users by means of special biometric devices.

Input of the identifier and the password by the user is processed more often from the keyboard. However many modern protection systems also use other types of identifiers - magnetic cards, radio-frequency cards, smart cards.

Biometric methods are characterized by high level of reliability of the user identification. There is also possibility of errors of recognition (skip over or a false alarm) as well with higher cost of systems by itself.

Identification and authentication of users should be made at their each logon and at renewal of operation after a short-term break, after the non-active period.

2.2.2. Access differentiation of the registered users to computer network resources

Access control to computer network resources is such order of usage of resources of the automated system at which subjects get access to system objects in strict correspondence with the installed rights. Rights of differentiation of access are a collection of the rules regulating access rights of subjects to objects in a system.

Authorization of users is processed with usage of the following mechanisms of implementation of access differentiation:

- The mechanisms of selective access control grounded on usage of attribute charts, lists of permissions, etc;
- The mechanisms of proxy access control grounded on usage of labels of confidentiality of resources and levels of users tolerance;
- Mechanisms of support of the closed environment of the entrusted software (individual lists for each user of the programs resolved for usage), supported by users' mechanisms of identification and authentication at their logon.

Differentiation hardware of access to computer network resources should be considered as the constituent of the uniform monitoring system of users' access (Abalmazov E.I. 2007, pp. 69-78):

- On controllable territory;
- In separate buildings and organization branches;

- To network units and protection system units of an information (physical access);
- To informational and network software resources.

Access control mechanisms of users to access objects fulfill a dominant role in support of internal security of computer systems. Their operation is based on the concept of the uniform access manager. The essence of this concept consists the access manager appears as the intermediary-controller at all calls of subjects to objects.

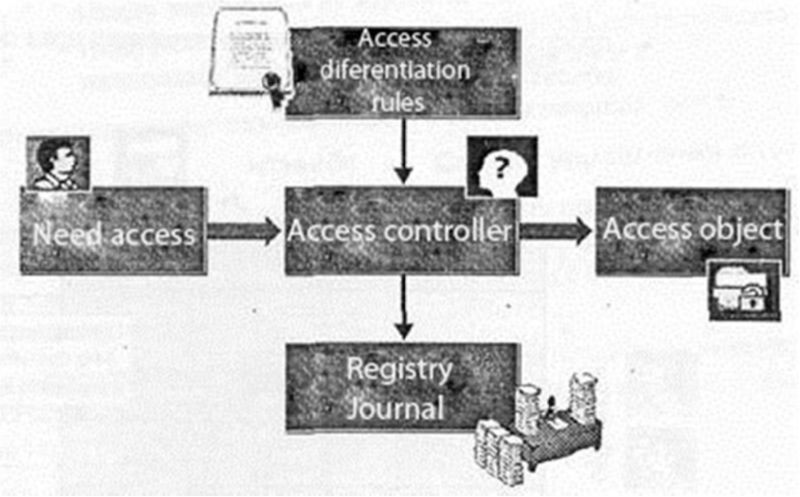


Fig. 2.2. The diagram of operation of the access differentiation mechanism.

Abalmazov(2007, pp. 76-78) points out the main functions of access manager:

- Checks access rights of each subject to the concrete object on the basis of the information containing in a database of a protection system;
- Resolves or prohibits (locks) access of the subject to the object;
- If necessary registers the fact of access and its parametres in system log (including attempts of unauthorized access with excess of rights).

The main requirements to implementation of the access manager are:

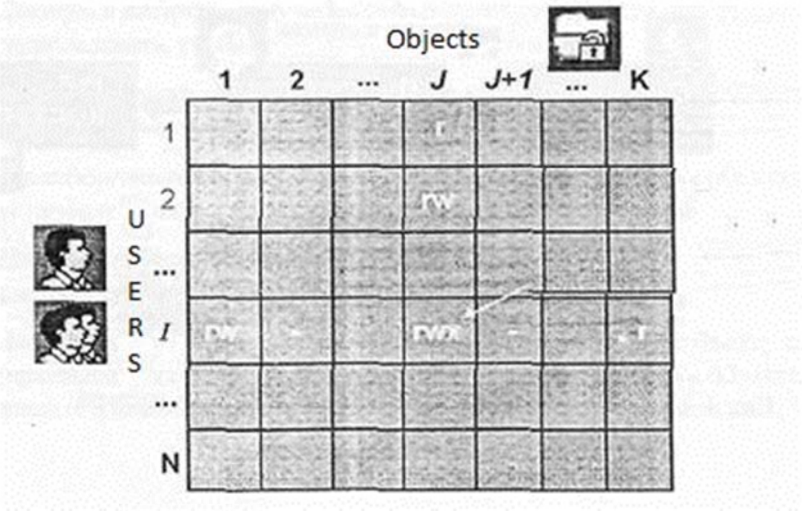
- Entirety of controllable operations (to check all operations of all subjects over all objects of system should be exposed, - manager detour is supposed impossible);
- Possibility of formal validation of functioning;

- Minimization of resources used by the manager.

In a general view operation of access differentiation of subjects to objects is based on check of data, which is being kept in a security database. As a security database understand a database storing the information on access rights of subjects to objects. For modification of a security database of access differentiation should include resources for exclusive users (security managers, owners, etc.) on conducting this base. Such controls for access should provide possibility of performance of the following operations:

- Additions and removals of objects and subjects;

- Review and change of appropriate access rights of subjects to objects.



	1	2	...	J	J+1	...	K
1				r			
2				rw			
...							
I	rw	-		rwx	-		r
...							
N							

Fig. 2.3. A matrix of selective access control (Abalmazov I.E. 2007, p. 90)

The basis of access differentiation database resources is made generally by an abstract matrix of access or its real representations. Each string of these matrixes corresponds to the subject and a column - to network system object. Each unit of this matrix represents the arranged collection of values, defining access rights (for all possible access modes - reading, modification, removal, etc.) the certain subject to the certain object.

2.2.3. Registration and the immediate notification about safety events

Registration methods are intended for reception and accumulation (for the purpose of the subsequent analysis) to a state information of system resources and about operations of the subjects recognized as system administration potentially dangerous to system. The analysis of the registration of the information gathered by resources allows eliciting the facts of violations, effects on system and define how far violation has come, to prompt a method of its investigation and searching ways of the infringer and correction situation.

In addition, registration resources allow receiving the exhaustive statistics on usage of those resources, the internetwork traffic, usage of tools, unauthorized access attempts, etc.

Except record of data on specific events in special logs for the subsequent analysis of a registration resource of events can provide and the real time notification of safety managers about state of resources, attempts of unauthorized access and other violation.

According to Abalmazov(2007, p. 102) at registration of safety events in system log the following information is usually collected:

- Date and time;
- The identifier of the subject (the user or software), carrying out that operation;
- Operation by itself.

Registration mechanisms are very closely linked to other protective mechanisms. Signals about occurring events and the detailed information on them receive registration mechanisms from control mechanisms (subsystems of differentiation of access, the control of resources integrity and others).

In the most developed protection systems the notification subsystem is interfaced to mechanisms of operative automatic reaction to specific events. Abalmazov(2007, p.108) carried out the main ways of reaction to detected facts of unauthorized access, they can be supported by:

- Alarming feed;
- Safety manager notification;
- Notification to the owner of the information in that system;
- Removal of the software (processes) from further performance;
- Disconnecting (blocking) terminal or computer from which attempts unauthorized access to the information;
- Ban the infringer from the list of the registered users, etc.

2.2.4. Cryptography methods of information protection

Cryptography methods of protection are based on possibility of realization of some operation of conversion of the information which can be fulfilled by one or several users of the system possessing some secret key without which it is impossible to carry out this operation.

In classical cryptography method one unit of the classified information is a key the knowledge of which allows the sender to crypt the information and to the receiver to decrypt it. These operations of enciphering with a high probability it is impracticable without knowledge of a private key. As both sides owning a key, can both to cipher, and to decrypt the information, such algorithms of conversion name symmetric or algorithms with the confidential key.

In cryptography with an open key two keys are available, at least one of which it is impossible to calculate from another. One key is used by the sender for the information encryption which is necessary to provide. The other key is used by the receiver to decrypt the received information. There are applications in which one key should be unclassified, and another - confidential. Algorithms of conversion with opened and confidential keys name asymmetric as roles of the sides owning different keys from pair are various.

Cryptography methods are generally concern:

- Encryption (decryption) information;
- Creation and check of the digital signature of electronic documents.

Domarev(2006, p. 144) Application of cryptography methods and resources allows providing solution of the following tasks on information protection:

- Preventing of possibility of unapproved acquaintance with the information at its storage in the computer or on alienated carriers, and also by transmission on data links;
- Confirmation of authenticity of the electronic document, the proof of authorship of the document and the fact of its reception from an appropriate source of the information;
- Support integrity guarantees - exception a possibility of unapproved change of the information;
- The strengthened authentication of system users - owners of private keys.

The main advantage of cryptography methods of protection the information is that they provide the high guaranteed protection, which can be calculated and expressed in the numerical form (an average of operations or necessary time for disclosure of the crypted information or keys).

Domarev(2006, pp. 152-154) points out the main disadvantages of cryptography methods:

- The big expenses of resources (time, productivity) on performance of cryptography conversions of the information;
- Difficulties with sharing of the crypted information;
- High requirements to safety of private keys and protection of open keys against substitution;

2.2.5. The control of integrity and authenticity of the data transferred on data links

The electronic digital signature is the string of characters received as a result of conversion in hardware of certain information content on mathematical algorithm with usage of keys, having an invariable relation with each character of the given information content.

Application of the electronic digital signature allows (Meshcherjakov V. A. 2006):

- Providing authenticity of the information;
- Providing the integrity control (including the validity) of the information;
- Dealing with a question on the legal status of the documents received from automated system.

Methods of the integrity control of system resources are intended for timely detection of system resources modification. It allows providing stable functioning of a protection system and integrity of the processed information. The integrity control of the software, the processed information and protection frames, for support of an invariance of the software environment defined by provided technology of processing, and protection against unapproved adjustment of the information should be provided:

- Resources of access differentiation , prohibiting modification or removal of a protected resource
- Resources of matching of critical resources with their standard copies (and restoring in case of integrity violation);
- Resources of count of check sum (signatures, etc.);
- Resources of the digital signature.

The internetwork screens installed in connection points with the Internet - provide protection of external perimeter of a network of firm and protection of the own Internet - the servers opened for the common using, from unauthorized access. The main protection methods are (Galatenko V.V. 2009):

- Translation of addresses for hiding of structure and addressing of an internal network;
- Filtering of the traffic;
- Handle of access lists on routers;
- Additional identification and authentication of standard services users;

- Contents audit of informational packages, revealing and neutralization of computer viruses;
- Virtual private networks (for protection of the data flows transferred on open networks - confidentiality supports, - are applied the cryptography methods considered above);
- Counteraction to attacks to internal resources.

2.3. Handling of protection methods.

The competition in the field of security system development of computer systems inevitably leads to unification of the list of the common requirements to such resources. One of items in such unified list practically always can have the requirement of controls for all available protective mechanisms. Unfortunately, developers of security systems give main attention to implementations of protective mechanisms, instead of controls for them. Ignorance, misunderstanding or underestimation by most designers and developers of the psychological and technical obstacles arise at implantation of developed protection systems. To overcome successfully these obstacles is possible only by having provided necessary flexibility of handling those protection systems.

The insufficient attention to problems and wishes of customers, to support the convenience operation of security often is a cause of refusal of using concrete protection systems.

In our days in most cases installation of protection frames is made on already functioning computer systems. Protected computer system is used for solution of the important applied tasks, in a continuous work cycle, most owners and users extremely negatively concern any, even short-term, breaks in its functioning for installation and customization of protection frames or partial loss of working capacity of system caused by incorrect operation of protection frames.

Implantation of protection frames becomes complicated because correctly customize security system is impossible to make at the first time. Usually it is caused by absence for the customer of complete detailed list of all protection hardware, software and informational system resources and the ready list of the rights of each user access to system resources.

Therefore, the stage of implantation of protection frames to some includes operations on initial revealing and respective alteration of customizations of protection frames. These operations should pass for owners and users of system as less troubles as possible.

It is obvious that the same operations frequently should be repeated by security administrator and at an operation phase of system each time at changes of structure of hardware, the software, staff and users etc. Such changes occur often enough; therefore protection system controls should provide convenience realization of changes of customizing a protection system necessary thus. If the protection system does not consider this dialectics, it does not possess sufficient flexibility and does not provide convenience change-over such system becomes not the assistant, but only troubles for everything including administrators very fast.

Those solutions which are comprehensible to one stand-alone computer or a small network from 10-15 workstations, do not suit serving staff at all (including administrators) from big networks with hundreds of workstations.

To solve the problems of handle by protection frames in the big networks system it is necessary to provide the following possibilities:

- Possibilities of handle by protection mechanisms in on-line mode (far off, from a workstation), and locally (direct from a concrete workstation) should be supported. And any changes of customizations of the protective mechanisms, made on-line, should extend automatically on all workstations which they concern (irrespective of a state of a workstation at the moment of modification of the central database). Similarly, the part of the changes made locally, should be automatically mirrored in the central database of protection and if necessary also is dispatched on all other servers which they concern. For example, change of the password by the user, carried out on one of the workstations, the new value of the password of this user should be mirrored in the central database of protection of a network, and also dispatched on all workstations on which user is going to work;

- Handling the protection mechanisms of the concrete server should be carried out independent from server’s activity. After inclusion of the inactive server all changes of the customizations, protection concerning of its mechanisms, should be automatically transferred on it.

- In large systems upgrading the protection frames demands from serving staff of the big expenditures of labor and is linked to necessity of detour of all workstations for reception to them of local access. Carrying out of such replacements can be called as necessity of elimination of the detected installation errors, and requirement of perfection and system development (installation of the new improved versions of software);

- For big computer networks special importance is gained by the operative control over a state of workstations and operation of users in a network. Therefore the protection system should include a subsystem of the operative control of a state of workstations of a network and tracing in the structure behind operation of users.

3. DEVELOPMENT OF THE COMPLEXITY OF RESOURCES PROVIDING SAFETY OF THE COMPUTER NETWORK

3.1. The description of a local area network of the company "NPP Inteps”

Let us consider a local area network of the company "NPP Inteps”. This company specializes in development and production of modern uninterruptible power supplies. The company is located in Lomonosovsky area of Saint Petersburg region and has several industrial premises. With about 40 engineers and programmers. Their primary goals are development and testing of new models of the uninterruptible power supplies and also creation of the software for those supplies.

By development of a local area network for that company it was necessary to consider some features of usage of computer equipment. The matter is that at that center developers of the new equipment and programmers use computers. If programmers are occupied by operation on the PC all the time and have properly equipped places, engineers use computers from time to time, first of all for analyzing calculations, working drawings, operations on testing from developed products. In total in the branch five stationary computers and 22 portable are involved.

Sending each other working drawings, thumbnails and the settlement files fulfilled in such programs, as AutoCAD, SolidWork and MathCAD, and also review of e-mail and materials in the Internet was the main way of data exchange inside the company. The size of transferred materials actually appeared insignificant and there is not increase of usage that’s why high requirements to a network were not shown. The network has been developed with usage of the equipment HomePlug AV that should provide a real transfer rate on a local area network to 85 Mbit/seconds. The following has been used at network creation engineering canter of the company "NPP" Inteps”:

1. The building is connected to industrial transmission lines.
2. In a building two parallel outlines of power supplies – a user's outline (sockets 220 V) and an outline providing power supply of lighting instruments are actually selected. The second outline passes under a building ceiling.
3. Conducting in a building is fulfilled in the hidden way in walls, the aluminum wire was used.

The circuit of electro support of an engineering center building is presented more low in a figure 3.1. The following denotations are used:

□ - Desktop

▭ - The computer (as we see, not on all desktops there is a necessity of usage of computers)

ƷƐ - The entry transformer

✕| - The wall lights

✕ - The ceiling lights

⏚ - Grounding

═ - Two-phase electrical line, 220 V

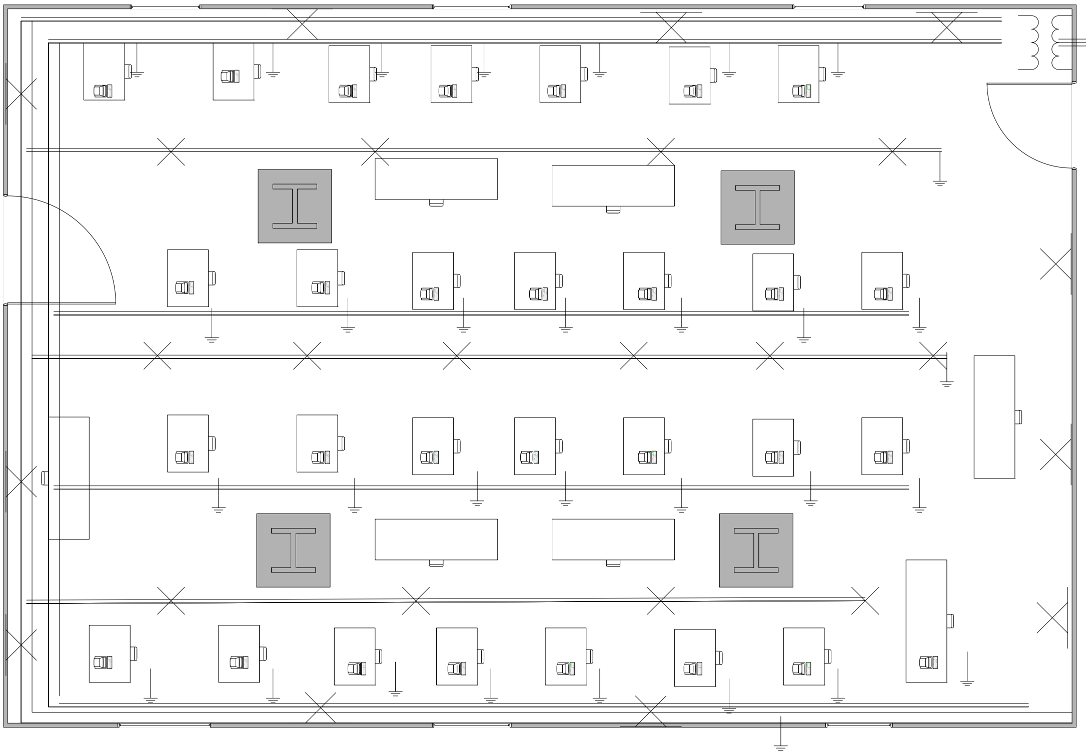


Fig. 3.1 The plan of engineering center building electro support

In this case for implementation PLC network in a building following main approaches have been used:

1. PLC network uses as the carrying environment only the lower outline of power supplies

2. The technology of a network – the bus with usage of the dedicated server providing access to the Internet, a mail server fulfilling function and a file server. On the same computer the auxiliary software for support of informational safety of a local area network has been installed.

3. Power supply of devices on workstations is made from a network of the lower outline with mandatory usage diode filters at connection to an electrical network of each workstation. The filter and PCL adapter on workstations are connected separately that provides protection of a carrying network against the interferences generated on workstations of employees, in particular when personal computer and other devices were used.

For support of reliable operation of a network and an exception of negative effect of the interferences linked to usage on desktops of computers and other devices giving electromagnetic interferences, diode the filter is used on each workstation eliminating penetration of interferences in carrying network. The connection circuit is in a figure 3.2.

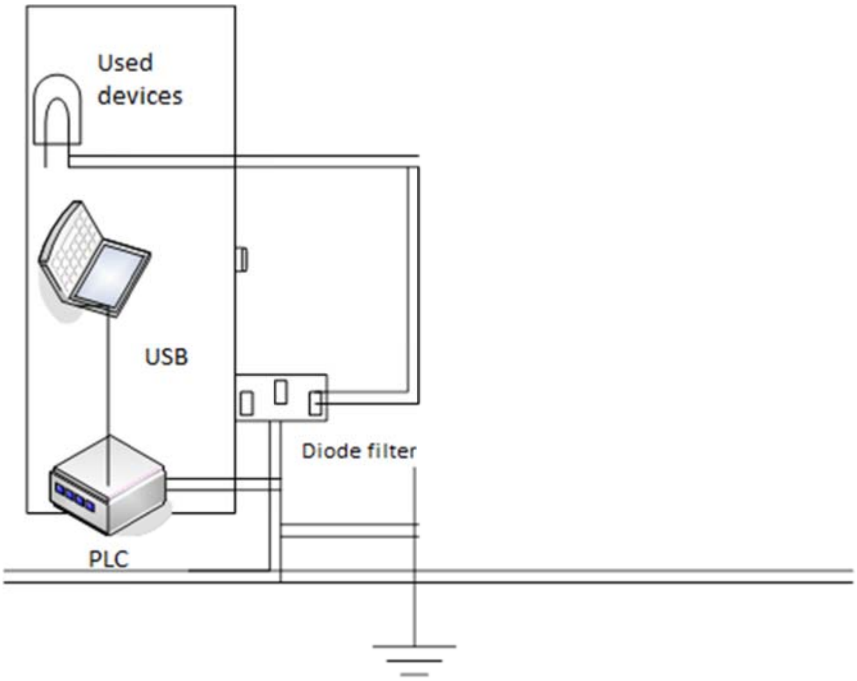


Fig. 3.2. The circuit of connection of terminals to PLC networks

The common circuit of a local area network is presented in figure 3.3.

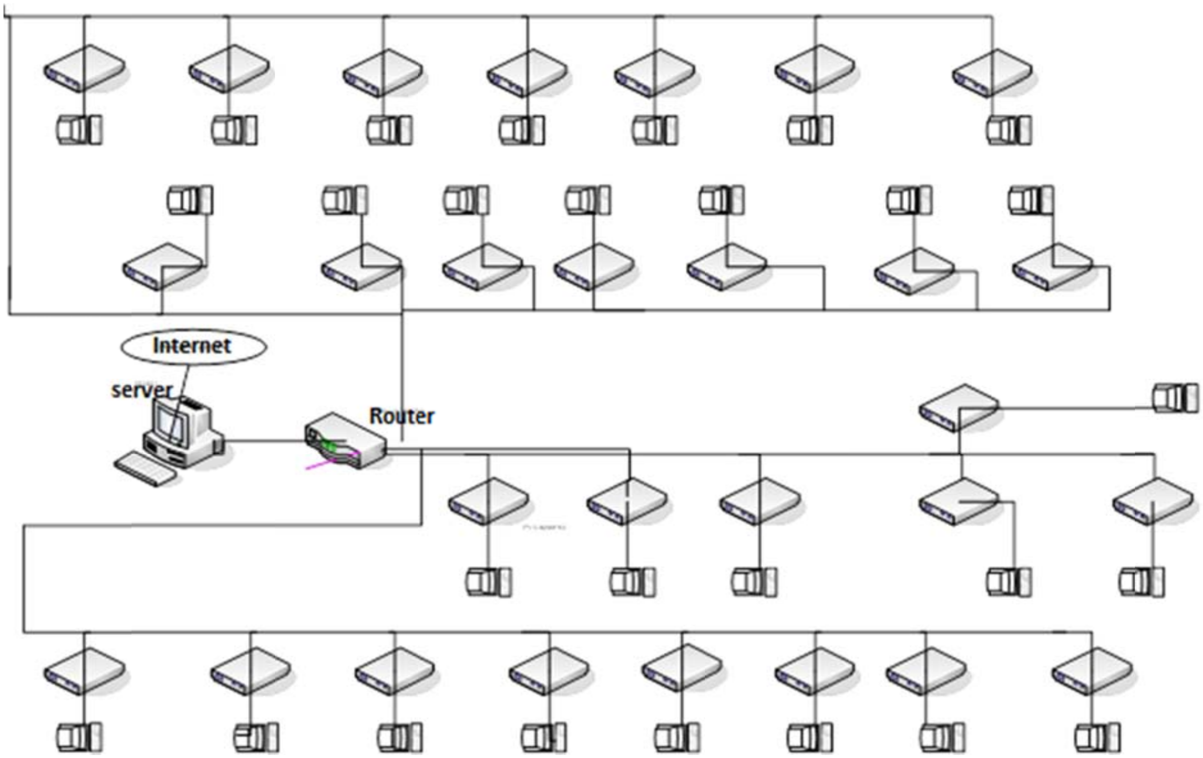


Fig. 3.3. The common circuit of a local area network of an engineering centre of "NPP Inteps”

3.2 The analysis of informational safety of a LAN in an engineering center of "NPP Inteps”

Next. the main threats of safety of a network and I will make guidelines on lowering of a level of threats are considered.

First, the main traffic in a network is formed by processes of an exchange by the working documentation used at designing and testing of new product samples in this company. The majority of documents are workers’ and do not represent interest for the third parties. However possibility of unauthorized access to the complete designer documentation can represent serious danger to the organization. The following requirements should be considered for a security policy in a local area network of the engineering center "Inteps”:

1. Exception of possible unauthorized access to the complete designer’s documentation

2. Support of integrity of information in a network

To consider only cases of unauthorized access with direct network connect (for the purpose of interception of the information, data corruptions, implantations of viruses, etc.) protection methods are comlited with usage of the same soft and hardware.

1. Network access with usage electromagnetic radiation and interferences

The network is physically organized in a separate building in the industrial the territory of the firm. The territory is guarded; therefore access of extraneous persons on territory is complicated. Building power supplies are carried out through reducing transformer that eliminates the possibility of network connect through wires out of a building.

In a building by operation on computers no special devices are used shielding radiation from screen monitors of the PC and other electromagnetic interferences. However territorial allocation of buildings in guarded territory and absence of places of direct visual contact within reasonable visibility out of territory makes almost impossible data read-out from screens of computers or interception electromagnetic interferences by operation on the keyboard, etc. Besides, it should be considered that the notebooks with the LCD-monitors have very low level of radiation and this makes any interference impossible

It is also necessary to mark that each workstation in a network is grounded that according to reasoning in paragraph 2.2. assume connection of protective grounding to each unit of a local area network through the filter which possesses the big resistance in a wide band, but a small resistance on frequency of 50 Hz. The given circuit of connection essentially allows lowering the level of magnetic radiation of the on-line computers that is especially important, as, unlike classical networks, the networks constructed on PLC technology, use unshielded cable as the physical environment of transmission.

Nevertheless, the difficult structure of electro conducting in a building theoretically admits hidden connection to a network or directly through conducting or allocation in immediate proximity to conducting of the devices which are carrying out interception of induced electromagnetic radiations. There is a problem of unauthorized access to a network in connection with these.

2. Unauthorized access to a network.

Without stopping separately on ways of protection against unauthorized access to informational streams in a network with usage of terminals of a network (as resources of struggle against this threat are standard for all sorts of networks), we will consider in more detail the threats linked to unapproved network connect directly. In this case it is important, that the manager (or used for operative reaction to arising threats the control program) has received in time warnings of attack. In a LAN of the engineering center of the company the program of network monitoring Alchemy Aye is used which is carrying out in real-time mode monitoring of transferred packages on various sites of a network and, in case of detection of losses of packages or their delays, producing the warning on a file server. Let us mark that violation of transferred packages on one of sub-frequencies of a network the given frequency is locked temporarily also network adapters further use other carrier frequencies for sending/reception of packages. In total usage there are 1536 sub-frequencies (as developers of the standard declare, blocking to 50 % sub-frequencies should not affect speed of data exchange in a network) so it is difficult to expect that the malefactor can organize simultaneous attack with usage at least half of the frequency spectrum.

As additional protection in a network is used the special Alchemy Eye Noise Filter unit is used the operation is initiated directly by the program of network monitor in case of detection of potential external interference in network operation. This unit is a source of informational masking noise. Noise parameters are program optimized according to network parameters, noise transmission is carried on frequencies with a spectrum repeating a spectrum of the noise signal.

However, at network attacks in which course the considerable amount of sub-frequencies appears affected, the transfer rate of packages falls, and losses of packages start to exceed some critical value (set by the network administrator), network operation is going to be locked before elimination of sources of extraneous interference in network operation.

The given algorithm of protection will be fulfilled in any case regardless of the fact that was violation of regular operation of a network – unauthorized connection of peripherals to cable system or failures in power supplies as a result of external technological or natural accident.

3. Data corruption in a network, threat of the data loss

At gaining access to network access by the intruder probably carrying out of informational attacks, for example, sending in a network of redundant arrays of the information (an informational bomb), implantation of programs-viruses, etc.

However, at the network organized on technology PLC stability of a network to this sort of effects appears even more, than for the similar networks organized under classical circuits (for example, cable networks Ethernet). The matter is that at sending of "informational bombs” corresponding sub-frequencies immediately are going to be locked, and sent packages are going to be destroyed in such network.

Further, in PLC networks hardware enciphering of the transferred data with AES algorithm is being used. It eliminates transmission to networks unencrypted messages (that is usual practice in a LAN of standard Ethernet). As consequence, first, the malefactor will hardly achieve disclosure of the received data for a reasonable period without additional effect on a network, and, secondly, in case of implantation it will be necessary for malefactor to spend their enciphering to a network of the programs, and for this purpose it is necessary to take hold of enciphering keys that in case of not authorized network access hardly is possible. Thus, a local area network constructed on PLC technology, shows high stability to the external attacks routed both on reception of the information from a network, and on violation of operation of a network, corrupting of data in network.

The package filters used in computer network of this company carry out the analysis of the information of network and transport levels of model OSI. These are network addresses (for example, IP) the remailer and the receiver of a package of number of ports of the remailer and the receiver, flags of TCP protocol, option IP, types ICMP. Package filters will be organized by resources of routers. Regular resources of operating systems are often used.

Packages are checked on three chains of the rules configured by the manager. As the internetwork screen the first level in the computer network of the company "Inteps” OS Linux is used as first type internetwork screen, working on a filter principle. The circuit of its operation is presented further.

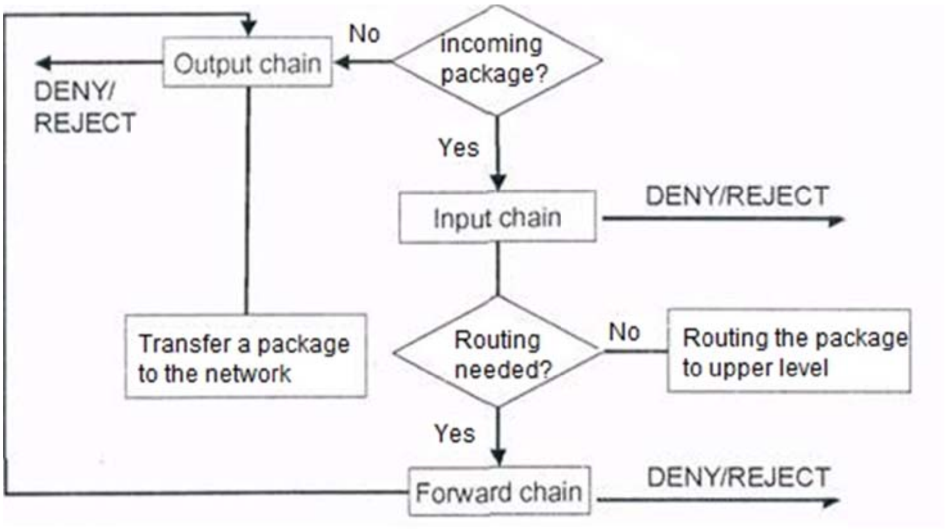


Fig. 3.4. A principle of usage of OS Linux quality of the package filter

This type of internetwork screen is grounded on usage of a so-called principle of mediating, i.e. the inquiry is accepted by internetwork screen, is parsed and only then transferred into a real server. Before resolve installation of TCP connection between computers of an internal and external network, intermediaries of level of connection firstly at least register the client. Thus does not very matters, from what side (external or internal) this client is. At positive result of registration between external and internal computers will organize the virtual circuit on which packages are transferred between networks.

As the gateway server of connection in the network of this company the gateway server with conversion IP - addresses is used (Network Address Translation, NAT). Application- level proxy servers, often named as proxy-servers, inspect and filter the information on a network application level. They differ on supported protocols of an application level. HTTP, FTP, SMTP, POP3/IMAP, NNTP, Gopher, telnet, DNS, RealAudio / RealVideo services are supported in computer network of this company. When client of internal network accesses, for example, to web server its inquiry gets to web intermediary (or it is intercepted by it). It establishes connection with a server from a customer name, and received information transfers to the client. For an external server the intermediary represents itself as the client, and for the internal client - as web server.

Based on technology of inspection of packages taking into account a protocol state, internetwork screen provides the highest level of safety. The method stateful inspection provides collection of the information from packages of the data, both communication, and an application layer that is reached by saving and its accumulation in special contextual tables which are dynamically refreshed. Such approach provides the greatest possible level of safety, inspecting connections at levels from 3 to 7 network models OSI whereas proxy intermediaries can inspect connections only on 5 - 7 levels.

Processing of new connection is thus carried out as follows:

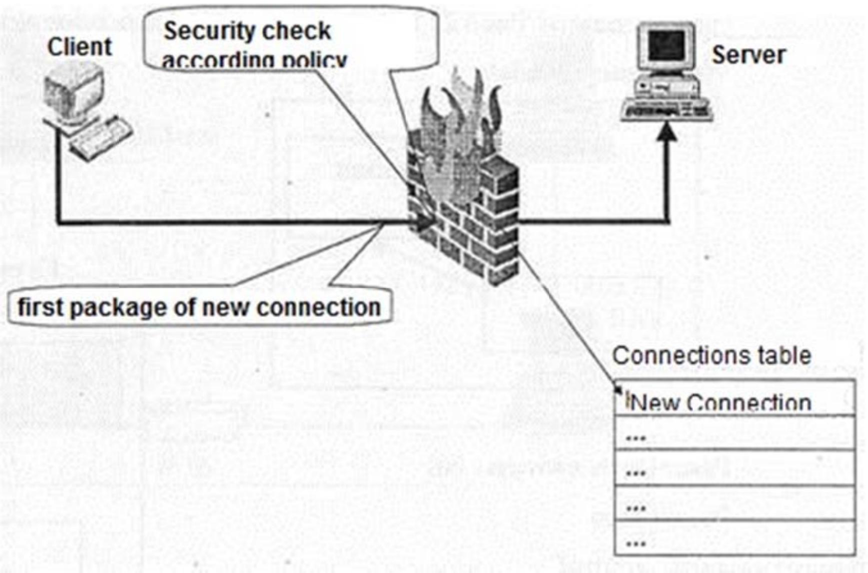

Client
Security check according policy
Server
first package of new connection
Connections table
New Connection
...
...
...
...

Fig. 3.5. Processing of new connection in company’s computer network

After connection is brought in the table, processing of the subsequent packages of this connection occurs on the basis of the analysis of tables.

In connection with the aforesaid it is possible to assert that PLC a building network engineering center of the company "NPP Inteps” differs high stability to external effects, and usage of hardware enciphering of high depth eliminates influence of the human factor by operation with the information demanding raised protection.

3.3 A policy of informational safety in the company "NPP Inteps”

For the direct organization (construction) and effective functioning of a complex protection system of the information in computer network of the company "NPP Inteps” the special service of safety of the information (the service of computer safety) should be created.

The service of computer safety represents the regular or supernumerary division created for the organization of qualified system development of protection of the information and support of its normal functioning.

It is necessary to assign solution of following primary goals to this division:

- Definition of requirements to a protection system of the information, its carriers and
Processing processes, security policy development;

- The organization of actions for implementation of the accepted policy safety, rendering of the methodical help and coordination of operations on to creation and development of a complex protection system;

- The control over observance of the installed rules of safe operation in the system, an estimation of efficiency and sufficiency of the accepted measures and applied protection frames.

The main functions of the service on Open Company "NPP Inteps” are listed in the following:

- Creation of requirements to a protection system at creation and development of the network system;

- Involvement in protection system designing, its trials and acceptance in maintenance;

- Planning, the organization and support of functioning of a protection system of the information in the course of functioning the network system;

- Training of users and staff of computer network to obey rules of safe information processing and service of components of the network system;

- Allocation between users of necessary accessories of accesses to resources of the network system;

- The control over observance by users and staff of network of the installed rules of call with the protected information in the course of its automated processing;

- Interaction with responsiblity for safety of the information in divisions;

- Regulation of operations and the control over managers of databases, Servers and network devices (for the employees providing correctness of application available as a part of OS, a DBMS, etc. resources of differentiation of access and other protection frames of the information);

- Acceptance of measures at attempts to the information and at violations of rules of functioning of a protection system;

- Observation of system operation of protection and its units and the organization of checks of reliability of their functioning.

Organizational-legal status services of safety of the information of the company "Inteps” is defined as follows:

- The service should submit to the chief of security service of this company, i.e. that person which bears personal responsibility for observance of rules of call with the protected information;

- Employees of the service should have the right of access to all premises where network equipment is installed, and right to demand from a manual of divisions of the termination of the automated information processing in the presence of direct threat for the protected information;

- The right to prohibit inclusion in number operating new computer network units if they do not meet the requirements of protection of the information should be given the head of the service of protection and it can lead to serious consequences in case of implementation of significant threats of safety;

- Number of the service should be sufficient for performance of all enumerated above functions;

- The regular staff of the service should not have other duties linked to network functioning;

- To employees of the service all conditions necessary for them for performance of the functions should be provided.

For the problem solving, assigned to division of safety of the information, its employees should have the following rights:

- To define necessity, to develop to represent on negotiation and the statement a manual the standard and organizational-administrative documents, safety of the information concerning questions, including the documents regulating activity of employees of other divisions;

- To receive the necessary information from employees of other divisions concerning application of information technology and maintenance computer networks, regarding concerning responsibilities of end-user;

- To participate in study of technical solutions concerning responsibilities of end-user at designing and development of new subsystems and complexes of tasks;

- To participate in trials of the developed subsystems and complexes of tasks concerning an estimation of quality of implementation of requirements on responsibilities of end-user;

- To inspect activity of employees of other divisions of the organization concerning rules of end-users.

Naturally, all these tasks are not under force to one person, especially in such large organization, as the company "NPP Inteps”. Moreover, the service of computer safety can include employees with different functional duties. The structure of this division should include the following experts:

- The head that is directly responsible for a state of informational safety and the organization of operations on creation of complex protection systems of the information in computer network;

- Analysts concerning the computer safety, states of informational safety responsible for the analysis, definition of requirements to security of various computer network subsystems and paths of support of their protection, and also for development of necessary is standard-methodical and organizational-administrative documents concerning information protection;

- Managers of protection frames, the control and the handles which are responsible for support and administration of concrete protection frames of the information and resources of the analysis of security of subsystems;

- The managers of cryptography protection frames responsible for installation, customization, removal crypto security, generation and allocation of keys, etc.;

- Responsible expert for solution of questions of protection of the information in developed by programmers and inserted applications (participating in development of requirement specifications concerning information protection, in a choice of resources and methods the protection participating in trials of new applications for the purpose of check of performance of requirements on protection etc.);

- Experts in protection of the information from leak on technical channels;

- Responsible rcpert for the organization of confidential office-work, etc.

3.4. A technique of implementation of safety policy of information in company "NPP Inteps”.

Now we will consider the purposes of informational safety in "NPP" Inteps”:

Confidentiality - support by the information only those people who are authorized for reception of such access. Storage and review of the valuable information only those people that are under the official duties and powers is intended for this purpose.

Integrity - maintenance of integrity valuable and the classified information means that it is protected from unauthorized modification. Existing set types of the information which have value only when we can guarantee that they are correct. The overall objective of an informational security policy of the company should guarantee that the information has not been damaged, destroyed or changed in any way.

Suitability - support of that the information and intelligence systems were accessible and ready for operation always as soon as they were required. In this case, the main objective of an informational security policy of company should be a guarantee that the information is always accessible and is supported in a suitable state.

The continuity of process of computer network functioning of firm and timeliness of restoring of its working capacity is reached:

- Carrying out of special organizational actions and development of organizational-administrative documents concerning support of computing process;

- Strict regulation of process of information processing with application of the computer and operations of staff system, including crisis situations;

- Assignment and preparation of the officials who are responsible for the organization and realization of practical actions for safety of the information and computing process;

- Accurate knowledge and strict observance by all officials using computer devices in the network, requirements of supervising safety documents;

- Application of various ways of backup of hardware resources, standard copying program and insurance copying of informational system resources;

- Constant maintenance of necessary level of security of components of system, continuous handle and management support of correct application of protection frames;

- Carrying out of the constant analysis of efficiency of the accepted measures and applied ways and resources of safety of a network, development and implementation of sentences on their perfection.

In the concept of informational safety of this company the following questions should be mentioned:

- Characteristic of computer network in the organization, as object of informational safety (protection object):
- Assignment, the purposes of creation and maintenance computer network of firm
- Structure and allocation of basic network elements of the organization, informational links with other objects
- Categories of the informational resources which are subject to protection
- Categories of the expert users of the organization, modes of usage and access levels to the information
- Interests mentioned at maintenance the expert of the organization of subjects of informational ratios;
- Vulnerability of the main components of the organization
- The purposes and tasks of support of informational safety of the organization and the main paths of their reaching (protection system problem solving)
- The list of the main dangerous effecting factors and significant threats of informational safety:
- External and internal effecting factors, threats of safety of the information and their sources
- Deliberate operations of the indirect persons, the registered users and serving staff
- Information leakage on technical channels
- Informal model of possible infringers
- The approach to risk estimation in the computer network of the organization;

- Substantive provisions of a technical policy in the field of safety of the information of the company
- Principles of support of informational safety of the organization;
- The main measures and methods (ways) of protection against threats, resources of support of demanded level of security of resources:
- Organizational (management) measures of protection
- Structure, functions and powers of division of support of informational safety;
- Physical protection frames
- Technical (hardware-software) protection frames
- System control of safety of the information
- The control of a system effectiveness of protection
- Prime actions for safety of the company’s information
- The list of the standard documents regulating activity in the field of information protection

4. CONCLUSION

In the near future the progress in the field of development of computer aids, the software and network technologies will impulse to development of resources of safety that will demand in many respects reconsidering an existing scientific paradigm of informational safety. New view substantive provisions on safety should be:

- Research and the analysis of causes of infringement of safety of computer systems;

- Development of effective models of the safety adequate to a modern degree of development program and hardware, and also to possibilities of malefactors;

- Creation of methods and resources of correct implantation of models of safety in existing methods, with possibility of flexible handle, safety depending on put forward requirements, admissible risk and expenditure of resources;

- Necessity of development of resources of the analysis of safety of computer systems by means of realization of test effects (attacks).

Wide information of societies, implantation of computer technology in sphere of handle of objects, prompt growth of rates of scientific and technical progress along with positive reaching in an information technology, create real premises for leak of the confidential information.

The main objective of the thesis was development of the common guidelines on information protection in computer networks and development information safety possibilities. The following results are received:

1. The main paths of protection against unauthorized access to the information circulating in processing systems are considered.
2. Classification of ways and information protection frames is made.
3. The analysis of security methods in processing systems is carried out in details.
4. The main directions of protection of the information in computer networks are considered.
5. The concept of safety of local area networks of engineering building of the company "NPP Inteps" and safety questions at group data processing in services and firm divisions are developed.
6. Framing of a security policy of concrete firm is carried out and the technique of implementation of this policy is given.
7. The information safety documents in the company "Npp Inteps" is developed.

REFERENCES

1 Abalmazov E.I., Method and technical resources of counteraction to informational threats. - "Grotech", 2007

2 Bezrukov N.N., Computer virus - Infra Th, 2007.

3 CSI/FBI 2005 Computer Crime and Security Survey, Computer Security Institute, 2005.

4 Devyanin P. N. Theoretical bases of computer safety: the Manual for high schools - Radio and link, 2007. P.N.Devjanin, O.O.Mihalsky, D.I.Pravikov, A.J.ShCherbakov

5 Domarev V.V. Zashchita information and safety of computer systems. - Publishing house "Diasoft", 1999. – p. 480.

6 FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems initial public draft version 1.0

7 Galatenko V.V., Informational safety, "Open systems", № 1, 2008.

8 Galatenko V.V., Informational safety, "Open systems", № 1, 2009.

9 Galatenko V.V., Informational safety, "Open systems", № 2, 2009.

10 Galatenko V.V., Informational safety, "Open systems", № 4, 2007.

11 Galatenko V.V., Informational safety, "Open systems", № 6, 2008.

12 Gerasimenko V. A. Information protection in the automated processing systems: 2004. – p.176.

13 Grinberg A.S., Gorbachev N.N., Tepljakov A.A.protection of informational resources: the Manual for high schools. - M: the UNIT-IS given, 2003. p. 327.

14 Gundar K..U Protection of the information in computer systems - «Korneichuk», 2005. K.J.Gundar, A.J.Gundar, D.A.Janyshevsky.

15 Hofman L, Modern methods of protection of the information, - Moscow, 2005.

16 ISO/IEC 13335-3 Information technology. Guidelines on handle of safety information security. Management methods safety

17 Jurasov J.V., Kulikov G. V, Nepomnyaschys A.V.method of definition of value of the information for estimation of risks of safety of the information. Safety of an information technology. 2005. №1. p. 41-42.

18 Levin A.N., information Protection in information systems and networks. - "programming", 2004

19 Meshcherjakov V. A. Methodical support of a substantiation of requirements to protection systems of the information from program - mathematical effect in the automated intelligence systems of critical application. Safety of an information technology Release 2, 2006, MEPhI. V.A.Meshcherjakov, S.A.Vjalyh, V.G.Gerasimenko.

20 Shankin G.P. Value of the information. Questions of the theory and applications. - Philomatis, 2007, - p.128.

21 The law «About the information, information and information protection».

22 Torokin A.A. Basics of technical protection of the information. - M: Publishing house "Os-982, 2003 - 336 with.

23 Walker of L, Blejk I, safety of the computer and the organization of their protection, - Moscow, 2001.