**NTNU – Trondheim**
Norwegian University of
Science and Technology

# Testing and verification methods to secure Industrial Control Systems (ICSs)

**Renaldas Skarnulis**

Master of Science in Communication Technology
Submission date: July 2020
Responsible professor: Peter Herrmann
Supervisor: Mate J. Csorba

Norwegian University of Science and Technology
Department of Telematics

**Title:** Testing and verification methods to secure Industrial Control Systems (ICSs)
**Student:** Renaldas Skarnulis

**Problem description:**

IT (Information Technology) and OT (Operational Technology) is converging inevitably and rapidly in critical infrastructures, such as the maritime transportation, oil and gas, renewable energy, and petrochemical industries. Legacy systems and industrial control systems that were designed and sometimes commissioned without cyber security in mind need to be protected from emerging security threats. Verification of OT cyber security by testing requires a blend of expertise between traditional IT security and very often experience with bespoke industrial communication systems. To help asset owners and operators within these critical infrastructure sectors, we have to develop and experiment with new methods and tools to test and improve their cyber security posture.

The expected outcome of the project will be to produce novel tools and methods for cyber security testing of ICSs.

**Responsible professor:** Peter Herrmann
**Supervisor:** Mate J. Csorba

# Abstract

With every year, the number of devices, connected to the Internet, increases in the world. Not only devices but also hackers becomes smart. Some create, others hack. And not all hackers use their business for good purposes. Therefore, special attention must also be paid to the protection of information systems.

In this work, we will focus on industrial control systems and their protection. We will get acquainted not only with how these systems work, what their meaning is in production, but also with an overview of the main threats, arising from possible security vulnerabilities and breaches. Here we will look at the history of successful hacked systems and the possible consequences for business and humanity.

To better understand how an intrusion into information systems takes place, we will look at it through the eyes of a hacker step by step. Only with a good understanding of how the hacking process takes place we can choose the right protection to prevent potential hacker hacking.

We will conduct a practical study of the potential threat to industrial control systems by looking for a vulnerable system on the Internet. In this way, we will check on testing and verification methods to secure industrial control systems, provide recommendations on which methods to test and how to protect information systems.

# Contents

# List of Figures

# List of Tables

# Acronyms

AES - Advanced Encryption Standard;
AS - Automated System;
AWS - Automated Workstation;
CIS - Corporate Information Systems;
CKC - Certification and Key Center;
DDBMS - Data Base Management System;
DDoS - Distributed Denial-of-Service;
DES - Data Encryption Standard;
DISS - Design of the Information Security Subsystem;
DLP - Data Loss Prevention;
DS - Digital Signature;
DSA - Digital Signature Algorithm;
ECDSA - Elliptic Curve Digital Signature Algorithm;
EDS - Electronic Digital Signature;
EPC - Event-Driven Process Chain;
ERP - Enterprise Resource Planning;
ES - Electronic Signature;
FP - Factorization Problem;
FSTEC - Federal Service for Technical and Export Control;
FTP - File Transfer Protocol;
HDD - Hard Disk;
HIDS - Host Intrusion Detection System;
HMI - Human-Machine Interface;
HTTPS - Hypertext Transfer Protocol Secure;
HW - Hardware;
ICS - Industrial Control Systems;
IDEA - International Data Encryption Algorithm;
IIPS - Integrated Information Protection System;
IKE - Internet Key Exchange;
IMS - Information Management System;
I/O - Input/Output;
IP - Internet Protocol;
IPS - Intrusion Prevention System;
IPSEC - Internet Protocol Security;
IS - Information Systems;
ISO standard - International Organization for Standardization;
IST - Information Social Technologies;
IT - Information Technology;
KCDSA - Korean Certificate-based Digital Signature Algorithm;

LAN - Local Area Network;
MD5 - message-digest algorithm;
MES - Manufacturing Executive System;
MPI - Multi Point Interfaces;
MSW - Malicious Software;
NESSIE - New European Schemes for Signatures, Integrity and Encryption;
NIDS - Network Intrusion Detection System;
NMC - Network Management Center;
OPC - Open Platform Communications;
OSI model - Open Systems Interconnection model;
OS - Operational Security;
OT - Operational Technology;
PC – Personal Computer;
PEC - Packet Error Checking;
PGP - Pretty Good Privacy;
PKI - Public Key Infrastructure;
PLC - Programmable Logic Controller;
P2P - Point to Point;
RAM - Random-access memory;
RSA - an abbreviation for the names Rivest, Shamir, and Adleman;
SCADA - Supervisory Control And Data Acquisition;
SEM - Security Event Management;
SHA - Secure Hash Algorithms;
SIEM - Security Information and Event Management;
SIM - Security Information Management;
SIM card - Subscriber Identification Module card;
S/MIME - Secure/Multipurpose Internet Mail Extensions;
SMTP - Simple Mail Transfer Protocol;
SQL - Structured Query Language;
SSH - Secure Shell;
SSL - Secure Sockets Layer;
STRIDE model - Spoofing, Tampering, Repudiation, Information disclosure (privacy breach or data leak), Denial of service, Elevation of privilege;
TCP - Transmission Control Protocol;
TLS - Transport Layer Security;
TP - Technological Processes;
UDP - User Datagram Protocol;
URL - Uniform Resource Locator;
USB - Universal Serial Bus;
VLAN - Virtual Local Area Network;
VPN - Virtual Privat Network;

# Chapter 1 INTRODUCTION

The relevance of the thesis work is that today information security is one of the most popular concepts, since modern life is very strongly connected with information technologies in their true sense and each of us has to protect our data. Security in information technology is understood as a set of measures and is perceived as a single system. Computer security can have different aspects, among which there are no more or less significant, everything is important here. You can't just take and give up part of some measures, otherwise the system simply won't work. And every resource in such a system, whether it be a computer or a company server, must be reliably protected. Also, the files themselves and the entire local area network (LAN) require protection. Access to all data is also better organized securely and all people working with information are a link in the chain of the mechanism that is responsible for the operation of the entire security system. Today, the information security market has many separate engineering, software, cryptographic, hardware solutions for the security of stored data.

In the literature on information protection there are many descriptions of methods and means based on them, as well as theoretical models for organizing protection. But in order to create optimal conditions for high-quality data protection in the company, it is important to combine individual security tools into a single system. It is important to understand that in it the main elements should remain a person. Moreover, this person is a key component, as well as the most difficult to formalize and weak link. The development of a data protection system (DPS) for a company is not the main task, such as making a profit or producing goods. Therefore, any DPS can not lead to large costs and difficulties in the work of the company. Nevertheless, it is obliged to ensure the proper level of protection of company information from all possible external and internal threats.

The main problem in the implementation of such protection systems is, on the one hand, the guarantee of reliable protection for all data stored in the system (the exclusion of any accidental or intentional receipt of data by third parties) and on the other hand, the inability of the protection system to create any noticeable problems for authorized users in the course of interaction with the resources of the system itself. Ensuring the desired level of security is a very complex problem that requires for its solution the implementation of joint scientific, technical, organizational and other measures aimed at creating an integrated system of organizational and technological solutions and the introduction of comprehensive data protection methods.

In this thesis, we will look at methods of bypassing systems security in network services and penetrating open information systems (IS). We can look for it by two sides. From one side we make an audit of security of information system, we look for possibilities to hack it and put into practice, and the other side - we do everything to protect the system. Tests on the use of this project during licensing will assess potential risks and reveal invisible problems.

There are three groups of people in the world who hacks IS - Black Hat, Gray Hat, White Hat [emp]. What is the difference? First are engaged in illegal hacking. Gray Hat hacks systems, but doesn't use it for bad purposes. They inform system owners of IS security vulnerabilities. Third - act within their rights. The question is, is it legal to hack IS?!

We will answer that it is legal in only two cases. First, when we try to hack our own IS. In the second case, when we have the written consent (agreement) from the organization about ongoing audit and hacking tests. These are the White Hack who are doing a full legal IS security audit. It should be mentioned that hacking is an illegal act, whereas a hacking test is legal. The difference is in the context in which the action is performed.

In terms of IS audit understanding, there is a big difference between a hacking and penetration tests. Auditing is used for legal purposes only. If hacking tests looks for vulnerabilities in the system security, then the audit presents weaknesses, problems of the IS, and suggestions to fix it. Hacking tests are based on the fact that the hacker doesn't have any information about computer networks, IS of the company. This method is called Black Box [Pos].

The aim of this thesis is to study the risks and threats associated with the information security of industrial control systems (ICS), to meet with testing and verification methods to secure ICS, industrial information systems and the subject of research is the enterprise information security system. Also - to develop a system of information protection in the industrial control system.

To develop a system of information protection in the industrial control system, it is necessary to solve the following tasks:

1) Consider the main problems, tasks and principles of information protection in computer networks;

2) Classify threats and vulnerabilities in computer networks;

3) To study and perform a comparative analysis of the main methods and means of protecting information in networks;

4) To develop terms of reference for the creation of an information protection system in intellectual property law and implement this system.

The other objectives of this project:

- Familiarize yourself with industrial networks, SCADA and management systems, as well as with relevant IT systems;
- Be able to work with tools and methods for testing OT cybersecurity. Together with the team at the DNV GL office in Trondheim, we will work on topics that can be applied in laboratories and possibly in the field through vulnerability assessments and penetration testing;
- Check the vulnerability of ICS systems and find gaps in information systems; - development of new tools and methods for testing cybersecurity ICS;
- Conducting surveys of individual companies, seeking information on cybersecurity and the experience of organizations in this area;
- Present conclusions, recommendations and suggestions on the results of the work performed. As a research method, the method of analysis of existing threats and information protection methods intended for use in industrial control systems, as well as the synthesis of the applied method to ensure an increase in the level of information security of the considered systems, is used.

When writing the thesis, such methods of scientific research were used as the study of scientific literature on the topic of research, the legal framework, analytical and comparative methods. The practical significance of the work lies in the possibility of using the developed proposals when introducing information protection tools in the information system of the enterprise in question.

Unfortunately, due to COVID-19, it was not possible to use DNV GL's laboratory for the practical part of this work, so together with the organization we found a common solution - to conduct a search for an insecure, vulnerable system on the Internet using the SHODAN search engine.

## 1.1 Motivation

Industrial Control Systems (ICS) security audits are for industrials, that have industrial control systems, SCADA systems, information systems, databases. This audit is required to address security vulnerabilities in ICS / SCADA and information systems. The audit identifies IS flaws, problems, and proposes to address them to prevent any potential ICS, IS hack, database, and information theft.

You can say why needs it (audit)?! Our company uses the latest information technologies and employs IT professionals.

But was the ICS security audit really done? Are employees really properly instructed on how to avoid IT disruption, information theft?

This can only be answered by an ICS security audit. Let's look at ICS hacking around the world, data theft in the last few years.

**BBC**: "Could hackers turn the lights out?" The attackers struck late in the afternoon on 23 December and used the remote access they had gained to computers in the control centre of power firm "Prykarpattyaoblenergo" to flip circuit breakers and shut down substations. That theoretical threat became all too real for more than 225,000 Ukrainians who were plunged into darkness by a sophisticated attack on one of the nation's power companies... https://www.bbc.com/news/technology-35204921

**The New York Times**: "A Cyber-attack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try." In August, a petrochemical company with a plant in Saudi Arabia was hit by a new kind of cyber-assault. The attack was not designed to simply destroy data or shut down the plant, investigators believe. It was meant to sabotage the firm's operations and trigger an explosion... https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html

There are many other examples of attacks that have already been carried out, but the consequences should be noted: disrupted businesses, consumer activity, stolen data, financial loss. Companies that experience hacking into information systems will inevitably suffer significant financial losses as they are disrupted, unable to produce products (services), employees are forced to wait for damaged information systems, databases will be reconstructed, and customers – when will be delivered products, rendered services.

Why did this happen and could these cyber-attacks be prevented?

These organizations really had security guards and IT professionals. Therefore, it is certainly an insufficient argument that using up-to-date information systems and having IT professionals will completely prevent cyber-attacks. Therefore, it is necessary to look at the vulnerability of ICS security, the shortcoming to eliminate problems and prevent cyber-attacks. This is the purpose of the industrial control systems security audit.

Remember: Secure industrial control systems - safe and successful business!

## 1.2 Objectives and scope

IT (Information Technology) and OT (Operational Technology) is converging inevitably and rapidly in critical infrastructures, such as the maritime transportation, oil and gas, renewable energy, and petrochemical industries. Legacy systems and industrial control systems that were designed and sometimes commissioned without cyber security in mind need to be protected from emerging security threats. Verification of OT cyber security by testing requires a blend of expertise between traditional IT security and very often experience with bespoke industrial communication systems. To help asset owners and operators within these critical infrastructure sectors, we constantly develop and experiment with new methods and tools to test and improve their cyber security posture [GL].

Basically, this project is divided into 3 parts - theoretical, practical and conclusions, recommendations, suggestions. The first part is a theoretical introduction to Industrial Control Systems (ICSs), principles of operation, terminology, gaps in ICS systems and security issues in dealing with breakthroughs, information systems security testing methods, and preparation for the practical part.

The second part is practical. This part will test ICS systems using various hacking tests by using hacking methodology. Gaps in information systems will be explored. To this end we will use the SHODAN web site, which is widely used to detect unprotected information systems, as well as ICSs, to conduct and describe other penetration tests.

The third part - conclusions, recommendations, suggestions. In this section, we will discuss previously performed penetration tests, their results, and make recommendations to protect ICS systems from hackers. The thesis will consist of the following parts:

1. The analytical part:

a.) Consideration of existing threats to information security;
b.) Analysis of existing information protection methods;
c.) Analysis of the features of information security in industrial control systems.

2. The practical part

a.) The choice of methods for protecting information in industrial control systems;

b.) The choice of information protection methods in industrial control systems;
c.) Comparison and selection of specific software products to improve information security;
d.) Development of organizational methods for protecting information.

## 1.3 Thesis Outline

The next chapters in this thesis are organized as follows:

- Chapter 2: Basic provisions of the theory of information protection on networks. In this chapter we will review the issues and challenges of information security in computer networks, what are the security principles and policies to protect information in the enterprise. We will also look at potential threats to the vulnerability of the corporate network.

- Chapter 3: Basic methods and means of protecting information on networks. This chapter introduces the legal, engineering, cryptographic methods and means, used to protect information in computer networks, and performs its comparative analysis.

- Chapter 4: Identification of the most relevant threats and selection of remedies. In this chapter we will review the main threats and vulnerabilities to industry control systems, we will look at the eyes of hackers as hacking, discuss the features of the implementation of information security systems, methods and means of ensuring the protection of information in ICS.

- Chapter 5: Introduction of an integrated information security system. In this chapter we will discuss measures to clarify the vulnerability and protection of information.

- Chapter 6: Practical part. The purpose of this chapter is to make an Internet survey to check the security of the Internet devices and to try to find a configuration vulnerabilities. This section presents the obtained research results and conclusions.

- Chapter 7: Conclusion. This chapter includes conclusion, made on the findings of this thesis and some recommendation for future works.

Chapter 2

# BASIC PROVISIONS OF THE THEORY OF INFORMATION PROTECTION ON NETWORKS

## 2.1 The main problems and tasks of protecting information in computer networks

Information security in computer includes a wide range of problems:

1) Ensuring data integrity - today all commercial information, accounting data, financial statements, customer bases, contracts, innovative ideas of employees, plans and strategy for its development are stored in a local information and computer network. Not always and not all documents are duplicated on paper, because the volume of information is very large. In such conditions, information security (IS) provides a system of measures, that are designed to provide reliable protection of servers and workstations from failures and breakdowns leading to the destruction of information or its partial loss. A serious approach to this issue means that information security should be based on a professional audit of the entire information technology (IT) infrastructure of the company. IT audit allows you to assess the status of the network and equipment, to analyse potential threats, to identify and timely eliminate the "weaknesses" in the cable system, server and workstations, disk systems and violations in the configuration of the equipment. Thus, the technical risks of a possible loss of information are reduced.

2) Ensuring confidentiality of information - protecting trade secrets directly affects the competitiveness of the company and its stability in the market. Here, information security is confronted with external and internal deliberate threats aimed at data theft. Hackers, industrial espionage and leakage of information through the fault of their own employees pose the greatest threat. The temptation to sell valuable commercial information is great not only for dismissed employees, but also for those whose ambitions in the workplace are unsatisfied. In this case, IS takes preventive measures aimed at controlling insiders and multi-stage protection of servers from hacker attacks.

Therefore, measures to combat unauthorized access should be aimed at achieving two goals:

1) Create conditions when random or deliberate actions leading to data loss become impossible. Information security solves this problem by creating a system of authentication and authorization of users, separation of access rights to information and access control;

2) Create a system in which employees or attackers could not hide the committed actions. Here, a security event monitoring system and audit of access to files and folders come to the aid of an IS specialist.

Effective means of protection against both external and internal threats are also: the introduction of a user password system, the use of cryptographic protection methods (especially for encryption) for particularly important information, the restriction of access to premises, the use of individual digital keys and smart cards, and the use of firewalls, installation of systems for protection against information leakage via e-mail, FTP-servers and Internet messengers, protection of information from copying. Currently, the number of incidents related to information security and violations of its requirements is increasing. An information security incident is the occurrence of one or more undesirable or unexpected IS events that are associated with a significant chance of compromising business operations and creating an IS threat [M.Aa], [Gal].

The organization of the incident response process has the following objectives:

1) To stop uncoordinated actions and to restore the efficiency of the entire company in the shortest possible time when an incident occurs;

2) To refute or confirm the fact of an IS incident;

3) Provide a full report on the incident and the necessary recommendations. Highlight the conditions for the accumulation and storage of accurate data on computer incidents. Implement a system for the rapid detection and/or prevention of similar incidents in the future (by analysing situations, that have already happened, changing IS policies, improving the IS system, etc.);

4) To maintain the safety and integrity of the facts of the incident. Implement the conditions for initiating a civil or criminal case against violators. Protect private rights, established by law;

5) To minimize possible violations of the operating procedure and data corruption of the IT system. Minimize the consequences of violating the secrecy, accessibility and integrity of the IT system;

6) Save the image of the company and its resources;

7) Train the company employees in the necessary actions properly to respond to the incident.

Information security incidents can be intentional or accidental (for example, be the result of some human error or natural phenomena) and are caused by both technical and non-technical means (ISO IEC TO18044-2007) (Figure 2.1). The consequences of the implementation of IS incidents can be events such as unauthorized disclosure or modification of information, its destruction or other events, that makes it inaccessible, as well as damage to the organization's assets or their theft. The most characteristic IS incidents are such as denial of service, collection of information, unauthorized access.

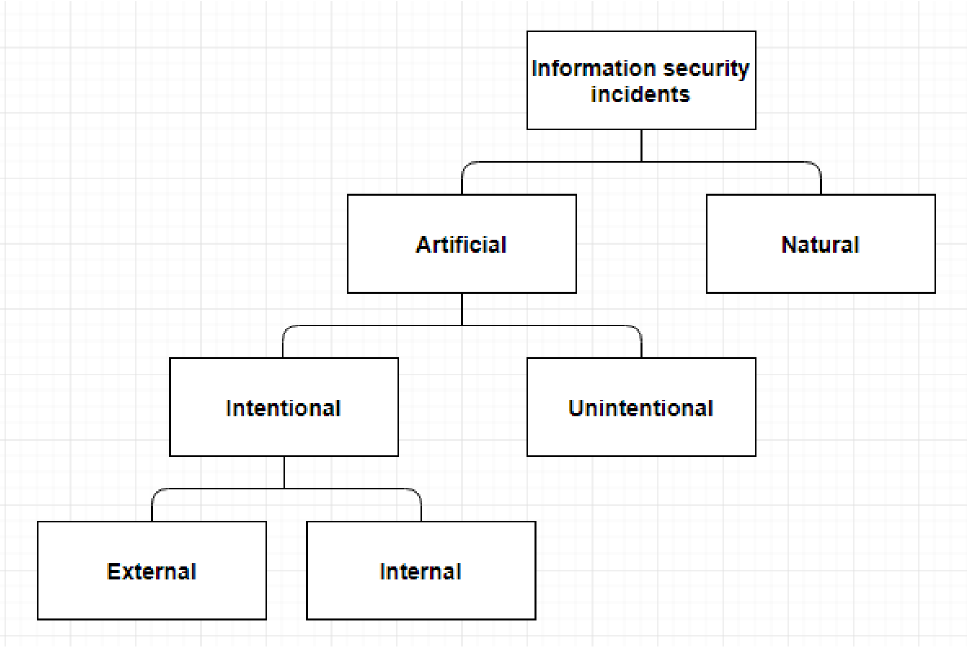


**Figure 2.1:** Classification of information security (IS) incidents [M.Aa]

For the assessment of security incidents and their detection in the information protection system, various techniques are applied, which will be discussed in the following paragraphs.

## 2.2 Basic principles and policy of information security of the enterprise

### 2.2.1 Information security principles

When building any system, it is necessary to determine the basic principles in accordance with which it will be built.

Integrated information protection system (IIPS) is a complex system that operates, as a rule, in the face of uncertainty, requiring significant material costs. Therefore, the definition of the basic principles of the IIPS will allow determining the main approaches to its construction [M.Aa], [ISA].

The following are the basic principles that can be attributed to any enterprise: state, commercial, mixed and other forms of ownership, as well as large, medium, small.

1) The principle of legality - here measures to ensure the functioning of the enterprise is developed on the basis and within the framework of existing legal acts. Legal acts of an enterprise must not contradict state laws and by-laws;

2) The principle of preventive (pre-emptive) - the content of this principle involves the timely identification of trends and prerequisites that contribute to the development of threats. Based on the analysis of these threats, appropriate preventive measures are developed to prevent the occurrence of real threats;

3) The principle of the validity of information protection - the implementation of this principle consists in establishing, through an expert assessment of the appropriateness of secreting and protecting this or that information, the likely economic and other consequences of such protection based on a balance of the vital interests of the state, society and citizens [AD], [Sys];

4) The principle of continuity - the protection of information occurs on a regular basis (constantly). Information protection is not a one-time event, but a continuous purposeful process that involves taking appropriate measures at all stages of the life cycle of an automated system (AS);

5) The principle of consistency implies the need to take into account all the interrelated, interacting and time-varying elements, conditions and factors that are significant for understanding and solving the problem of ensuring the safety of nuclear power plants;

6) The principle of complexity - at the disposal of computer security specialists there is a wide range of measures, methods and means of protecting computer systems.

Their combined use involves the coordinated use of diverse means in the construction of an integrated defence system that blocks all significant channels for implementing threats and does not contain weaknesses at the junctions of its individual components [G.G];

7) The principle of reasonable sufficiency - it is fundamentally impossible to create an absolutely insurmountable protection system. With enough time and money, any defence can be overcome. Therefore, it makes sense to talk only about some acceptable level of security;

8) The principle of economic feasibility - implies that the funds spent on protecting information should not exceed the cost of information [AD].

Among the principles considered, it is hardly possible to single out more or less important ones, and when building an integrated information protection system, it is important to use them together. In accordance with the international standard ISO / IEC 15408 [M.Aa], [HC], an organization's security policy is one or more safety rules, procedures, practices or guidelines that guide the organization in its activities.

The goal of creating a company's IS policy is to regulate IS management and support this process. An adequate level of IS can be ensured only on the basis of an integrated approach involving the use of both organizational protective measures and engineering and technical measures.

In modern practice of ensuring IS, the term "security policy" is used both in a broad and local sense. In a broad sense, a security policy is defined as a system of documented management decisions to ensure the IS of a company. In the local sense, security policy refers to specific documents for individual information subsystems or establishing clear rules in one given area of IS.

In accordance with international standards (for example, ISO / IEC 17799 [AD]), a security policy can regulate such means and methods of ensuring a company's IS as organizing protection (that is issues of responsibility for ensuring IS and coordinating the work of different departments of university), classification of resources and their control, physical protection, administration of computer networks, development and maintenance of IS, monitoring of compliance with established requirements, etc. The development of a security policy begins with the formulation of an exact statement of the goal of ensuring the IS of the company. At this stage, the first document related to security policy should appear - the concept of ensuring IS of a company, which defines a system of views on the problem of ensuring IS of a company and represents a systematic presentation of the goals and objectives of protection, the basic principles of its construction, organizational, technological and procedural aspects of ensuring IS.

### 2.2.2 Vulnerability classification

Modern information and computing systems basically have a set of software and hardware for organizing high-performance data processing and storage. Table 2.1 defines three classes of vulnerabilities: objective, subjective, and random [154], [inf].

| **Objective** | **Subjective** | **Random** |
|---|---|---|
| radiation technical communication facilities | software bugs | crashes and hardware failures |
| activatable | unskilled system management | Natural Aging Media |
| element base | misuse of hardware | related software crashes |
| features of the protected object | violation of the established access mode | power outages |
| features of the protected object | violation of the operating mode | communications damage |
| features of the protected object | violation of established security policies | damage to walling |

**Table 2.1:** Vulnerability Classification. [154], [inf]

Objective vulnerabilities directly depend on the features, capabilities and limitations of the technical characteristics of the equipment or system. Several types of vulnerabilities can be attributed to this class:

- Radiation of technical means of the system (sound, electromagnetic, electrical, etc.);
- Activated (these include, for example, illegal copies of software, software viruses that increase the risk of an attack, or directly trigger attacks, etc.);
- Features of the elemental base on which the system is built;
- Features of the protected object (location of the object, organization of channels, information transfer, etc.).

Subjective vulnerabilities are based on the human factor and directly depend on the actions of personnel, who have access and influence the operation of the IS.

Such vulnerabilities include:

- Software errors affecting the process of installation, operation and input-output of data;
- Unskilled system management;
- Improper operation of technical equipment;
- Violation of the established regime of access, security and protection of system objects;
- Violation of the operating mode of technical equipment;
- Violation of established security and privacy policies.

Accidental vulnerabilities arise, as a rule, due to force majeure circumstances (for example, natural aging and weather conditions). These events are difficult or impossible to predict. These include:

- Crashes and failures of technical means of the IS;
- Natural aging of storage media and data transmission media;
- Failures of related software (operating systems, database management software, antivirus programs, etc.);
- Power outages;
- Damage to life-saving communications;
- Damage to walling.

The complete elimination of first-class vulnerabilities is impossible. However, it is possible to dampen their impact by various technical methods for protecting IS. Vulnerabilities of the second class are eliminated by organizational and hardware-software methods. The vulnerabilities of the third class, by virtue of their nature, can only be partially "mitigated" through a set of organizational and engineering measures to ensure IS. A significant subset of vulnerabilities accounts for system security settings. Most often, security threats such as bookmark programs and viruses are mentioned in the literature.

A computer virus is a program that can infect other programs by modifying them with the addition of a copy of the virus or it's variant. A computer bookmark is a hardware and/or software tool that implements threats to computer hardware or software resources, using external functional objects that, under certain conditions (input data), perform actions that are not described in the documentation [G.G], [Lai].

### 2.2.3 Countermeasures to threats

Next, we consider the existing and proposed methods of countering these threats. Consider the methods of countering threats (table 2.2) arising from the vulnerabilities, listed in table 2.1.

| **Countermeasures** | **Threats** |
|---|---|
| **Obstacles** | Subjective: violation of the established access mode, violation of the operating mode |
| **Control** | Subjective: software errors, unskilled system management |
| **Regulation** | Objective: activated |
| **Regulation** | Subjective: violation of established security policies, violation of the operating mode, violation of the established access mode, improper operation of technical means |
| **Regulation** | Random: natural aging of storage media, crashes and failures of hardware, etc. |
| **Masking** | Subjective: violation of the established access mode, violation of established security policies |
| **Increased resiliency** | Objective: radiation of technical means of the system, element base, features of the protected object |

**Table 2.2:** Methods to counter threats. [G.G], [Lai]

The first column shows the methods, the second shows the vulnerabilities and the threats they protect against.

The main methods and means of information protection:

1) Obstacle: the prohibition of penetration into the territory of the computer network, access to equipment and storage media. Physical and hardware protections are used, for example, window grilles, security alarms, electronic key rings, etc.;

2) Management: regulation of system resources (databases, storage media, programs). The presence of the rules of users, technical personnel, programs. The protected system must be accompanied by actualized, complete documentation that allows for the development of the system and its qualified operation;

3) Regulation:

- Management of the list of individuals (users and maintenance personnel) admitted to the equipment;
- Limitation of the time of work with authorized terminals, restriction of access to system resources, restriction of tasks (procedures) allowed for execution;
- Regulation of places of permanent storage of information carriers.

4) Masking (encoding, encryption): data transformation in such a way that they become available only after the presentation of the key. It is possible to use steganography methods to hide not only the meaning of stored or transmitted information, but also the facts of its transmission and storage;

5) Increasing fault tolerance due to duplication (full, partial and combined) and noise-resistant coding of information, the use of adaptive schemes for organizing the system [A.Aa], [Pou].

The hardware means of information protection include technical solutions that are different in principle of operation and capabilities, which protect information from disclosure, leaks and unauthorized access. They are used in the study of technical means for the existence of information leakage channels, the search and detection of industrial espionage tools, countering unauthorized access to sources of confidential information, etc.

Software can be classified as follows:

- Self-defence tools included in the functionality, provided by the software developer;
- Protective equipment and standard devices;
- Means of identifying user privileges;
- Means of active protection in special circumstances, for example, in the case of an incorrect password, etc.;
- Passive protection equipment aimed at warning.

For example, there are three ways to protect against computer viruses:

- Scanners that scan protected areas of the computer system and test it for viruses;

- Resident monitors, located in the main memory and making sure that no unauthorized actions are performed in the system;
- Disk auditors working with a system snapshot and tracking changes.

The most effective means of combating viruses is prevention, which consists in using only licensed software, conducting regular backups, and checking all incoming information for viruses. Firewalls allow you to divide the responsibility zone into several parts and implement a set of rules for passing packets with data across the boundaries of the zones. Network packets can be filtered using firewalls at different levels of network interaction: firewalls can be classified into shielded routers, session-level gateways and application-level gateways. The former operates at the network level of the OSI model, but use information from the headers of the transport layer protocols in their work, filtering can be performed both by the IP addresses of the sender/receiver, and by the TCP and UDP ports. Do not protect against attacks with the substitution of connection participants. The latter operate at the session level of the OSI model and can also control transport and network information. They can control the installation of connections, check network packets. Still others can analyse packets at all levels of the OSI model, thereby ensuring the maximum level of protection, including through user authentication capabilities; verifying commands transmitted over application layer protocols; checking transmitted data for viruses and violating security policies [S.Vb].

However, firewalls do not provide complete protection against special software and hardware impacts. They are only able to detect about 30% of attacks on networks, connected to international information networks. The same applies to antivirus products. Currently, a common feature of modern security policy management systems is the ability to quickly create high-level and low-level security policies, distribute these policies to employees of the organization and monitor the facts of familiarization with and consent to the policies.

## 2.3 Classification and content of threats to software, vulnerabilities of corporate networks

### 2.3.1 Threats, affecting the organization

With the development of information and communication technologies, and increased access to the Internet, organizations become vulnerable to various types of threats their information is subjected to cyber-attacks. Threats come from various sources: employee activities or hacker attacks. According to the researchers [GS], [oEC], [A.Va], [A.Sb], [NJ], [LF], financial losses caused by security breaches are usually difficult to determine precisely, because a significant number of losses come from a small number of security incidents, which underestimates the IS risks systems [154]. As a result, managers must know the threats that affect the organization's assets and determine the degree of their influence, in order to know what they need to do to prevent attacks, and develop appropriate countermeasures.

Vulnerabilities are primarily vulnerable to system weaknesses that could be exploited by attackers and lead to dangerous effects. If there are vulnerabilities in the system, a threat can manifest itself through a threat agent by using a specific penetration method to cause unwanted effects [154], [A.Ab]. Moreover, financial losses of organizations can be significant.

According to the materials of the 11th annual conference on computer crime and security, 74.3% of the total losses are caused by: viruses, unauthorized access via laptops or mobile equipment, as well as theft of confidential information [S.Vb]. A study by McCue [A.Va] shows that 70% of fraud is perpetrated by insiders, not external criminals, but 90% of security tools focus on external threats. To find these threats, their sources and specific areas of the system that may be affected, IS assets can be protected in advance [154], [A.Ab]. Security threats can be observed and manifested in different ways, taking into account different criteria in relation to sources, agents and motivations.

Classification of threats helps to identify security threats in classes in order to analyse, evaluate their consequences and develop strategies to prevent or mitigate the consequences of threats in the system [M.Ac], [oEC].

The literature presents quite a lot of types of attacks on computer systems that are subjected to taxonomy in [M.Ac], [N.V], [A.Aa], [EN], [A.Ab], [A.E], [V.Aa]. The study showed that many authors have proposed taxonomies that allow classifying attacks based on their expected effect or denial of service [A.Aa], [EN], [A.E]. There are other approaches that include either the technique by which an attacker achieves the desired effect, for example, bypassing authentication, or the subject [154], [N.V], [A.Ab], [V.Aa]. We believe that it is necessary to introduce a hybrid threat classification model, based on a combination of both the threats themselves and their consequences in order to better determine the characteristics of threats and propose suitable countermeasures to reduce risks. A review of the literature showed that the following are the main principles of IS:

- The principle of mutual exclusion. Each threat in one category excludes all others, because the categories do not overlap. Each sample should correspond to no more than one category;
- The principle of comprehensive inclusion. Categories in the classification should include all possible options (all threat patterns);

- The principle of uniqueness. All categories must be clear and precise so that the classification is considered indisputable. Each category should be accompanied by an unambiguous criterion, that determines the need to include a threat in this particular category;
- The principle of repeatability. Repeated threat declarations should lead to the same classification, regardless of who carries out the classification;
- The principle of acceptance by the majority. All categories should be consistent with logic, be intuitive and practical, easy to be accepted by the majority;
- The principle of utility. Classification is necessary for use to understand the query field. It can be adapted to various application needs.

In general, these principles can be used to assess threats. A good classification should support the principles, presented [G.G], [GS], [oEC], [KN], [270].

A threat is an adversary's target and can be defined in two ways: through the methods that attackers use to exploit vulnerabilities in system components or through impacts on assets. Thus, threats can be divided into two main classes:

- Threats, based on attack methods;
- Threats, based on exposure methods.

First - consider the classification of threats, based on attack methods.

Ruf L. and colleagues [V.Aa] proposed a three-dimensional classification model of security threats. In this model, threats to space are divided into three groups (subspaces) in accordance with motivation, localization, and agents:

1) Threats to which agents' subject specific components of the system: human, technology and in accordance with the motivation of the threat can be divided into two groups: intentional and random;

2) In accordance with localization, threats are divided into internal and external;

3) In accordance with agents (components), threats can come from a person, technology (technic) and be caused by force majeure circumstances.

Geric S. and Hutinski Z. [154] proposed a hybrid model or C3 model, to classify threats to an information system. Three main criteria are used in this case [154]:

1) The frequency of occurrence of the threat;

2) The area of the threat (domain): physical security, personnel security, IS, operational security (OS);

3) Sources of security threats.

In [A.Ab], intentional threats are classified based on three factors:

- Preliminary knowledge of the attackers about the system: in terms of how much an attacker knows about the system with respect to its hardware, software, employees and knowledge users;
- Criticality of the area: it represents the criticality of parts of the system that may be affected by the threat;
- Losses: these are all losses that may occur in a system or organization (confidentiality, integrity, etc.).

Now we will try to provide the most complete classification of threats, associated with the danger of exposure (collision). The most common is the STRIDE model. Microsoft [A.Aa] and [EN] developed a classification method called the “step”, which is used in set and applications. STRIDE allows you to characterize known threats in accordance with the goals and objectives of the attacks (or the motivation of the attacker). A specific “step” of the step (its type) is formed from the first letter of each of the following categories: identity substitution, data forgery, refusal, information disclosure, denial of service and granting privileges. This goal allows you to create a rating of threats. The ISO standard (ISO 7498-2) listed five major security threats for exposure and services as a reference model [A.E]: destruction of information and/or other resources, corruption or modification of information, theft, deletion or loss of information and/or other resources, disclosure information, interruption of services.

Most security risk classifications are generally limited in using one or two criteria to classify threats. Others provide an unofficial comprehensive list of threats (not all threats covered by classification), and their categories are not mutually exclusive. This may be sufficient for a relatively stable environment when security threats are relatively stable, but in an ever-changing environment, organizations are not able to protect themselves even from internal threats [154].

Organizations are currently prone to several types of threats that affect their reputation, and it is important that they determine all the characteristics of the threats in order to mitigate their risks. It is believed that it is necessary to combine different classifications and create one - a hybrid. We will try to present it, observing all the principles of classification of threats. The main idea of our model is to combine most of the existing and previously described threat criteria and options for their potential impact. The list of classification criteria is as follows:

1) Source of security risk: internal or external;

2) Threats to the safety of agents: human, environmental and technological;

3) Threat motivation: targets attacking systems that may be malicious or non-malicious;

4) Intent of the threat: the purpose of the person who caused the threat may be intentional or the attack may be accidental. This criterion allows you to reconstruct the behaviour of the attack and determine the intent and harmfulness of the behaviour. Using this criterion allows investigators to help conclude the case with high accuracy and, therefore, reduce risks and accelerate decision-making for agent search [M.Ab];

5) Threat exposure: threat exposure is a security breach. The following consequences of threats were identified for our model: information destruction, information distortion, information theft/loss, information disclosure, refusal to use, elevation of privileges and illegal use.

To simplify the model, the binary sources of threats were used: internal and external.

Internal threats arise when someone makes unauthorized access to the network from any account on the server or physical access to the network. The threat may be internal to the organization as a result of the actions of employees or the failure of the organization process.

External threats may arise from individuals or organizations working outside the company. They do not have authorized access to computer systems or networks. The most obvious external threats to computer systems and resident data are natural disasters: hurricanes, fires, floods and earthquakes. External attacks occur through connected networks (wired and wireless), physical intrusions and partner networks.

In terms of agent threats, three classes are defined for our classification: people, natural disasters, and technological threats.

The proposed classification covers the full range of potential agents, since we include people, chemical and physical reactions to anthropogenic objects (technological), as well as natural for all those agents on which people have no influence.

**Threats to humans.** This class includes threats caused by human actions, such as insiders or hackers that cause harm or risk to systems.

**Environmental threats.** These are threats, caused unlike the human agent, by natural circumstances: natural hazards of natural disasters such as earthquakes, floods, fire, lightning, floods, wind, and, in addition, due to the behaviour of animals that cause serious damage to information systems. This class includes other threats, such as riots, wars, and terrorist attacks [V.Aa].

**Technological threats** are caused by physical and chemical processes. This applies to construction, design of premises. Physical processes include the use of physical means to obtain records in restricted areas, such as construction, connecting rooms, or any other designated area, theft or damage to hardware and software. Chemical processes include hardware and software technologies. This may include indirect support for the equipment system, for example, power [V.Aa].

**Threat motivation.** Attackers usually have a specific target or motive to attack systems. These targets can lead to harmful or harmless results.

**Malicious threats** consist of internal or external attacks, carried out by employees or non-employees, which can harm and “disrupt” an organization through various viruses. Malicious attacks are due to inappropriate policies and inadequate security controls that create vulnerabilities. This can be caused by the ignorance of employees, who are not intended to harm the system. The purpose of the threat is the intent of the person, who caused the threat. A deliberate threat is a decision in the form of harm to the organization. For example, this applies to computer crimes or when someone intentionally tries to harm property or information. Computer crimes include espionage, identity theft, child pornography, and credit card crime.

**Unintentional threats** are threats that are introduced unconsciously by harm. These threats mainly include unauthorized or inadvertent software changes. A random error includes data corruption, caused by programming errors by user errors or operator errors.

Thus, information security is an important problem for individuals and organizations, because it leads to large financial losses.

### 2.3.2 Threat risk management

The classification of threats is necessary in order to develop a general and flexible model that allows you to better understand the nature of threats, develop appropriate strategies and solutions for ensuring IS to prevent or mitigate their consequences. Ensuring increased requirements for IS involves carrying out various activities at all stages of the life cycle of IT. The approval of these measures takes place upon completion of the risk analysis stage and the selection of protective measures.

The main component of these plans is the periodic verification of the existing regime of security policy, certification of IP (technology) for full compliance with the requirements of the selected security standard. All of the above is called risk management.

When implementing a full risk analysis, a number of difficult tasks need to be addressed. The risk assessment process is divided into several stages:

- Determining the resource and evaluating its quantitative indicators or identifying potential negative impacts on the business;
- Threat assessment;
- Vulnerability assessment;
- Assessment of already implemented and anticipated IS support tools;
- Risk assessment.

On the basis of risk assessment, the means that support the IS regime are determined. Resources that matter to the business and are vulnerable to vulnerabilities are at risk if there is a risk in relation to them. When assessing risks, the possible negative impact of unwanted incidents and the significance parameters of the selected vulnerabilities, as well as threats to them, are taken into account.

Resources are often divided into several classes: physical, software, and data. Each class has its own methodology for assessing the value of elements. To evaluate the value of resources, a suitable system of criteria is selected. In addition to the criteria that take into account financial losses, the company may have criteria showing:

- Damage to the company's reputation;
- Problems, associated with violation of applicable laws;
- Damage to staff health;
- Damage from the disclosure of confidential and personal data;
- Problems, associated with the inability to full fill the obligations undertaken;
- Damage from the reorganization of a company or activity.

Other criteria may apply depending on the focus of the organization. So, in government agencies, criteria can be used that reflect the areas of national security and international relations. It is also important to identify vulnerabilities - weaknesses in the security system that cause threats to occur.

To specify the likelihood of a threat being realized, we investigate a certain period of time, during which the resource is protected. The possibility that the threat will be realized is expressed by the following factors:

- The attractiveness of the resource (the parameter is taken into account when considering the threat of intentional exposure by people);
- Use of the resource to generate income (the parameter is taken into account when considering the threat of deliberate exposure from people);
- Using vulnerabilities to attack.

Today, a large number of threat assessment methods are known. Many risk analysis techniques have already been developed. The main sources of security threats in this company are [G.G]:

- Threats through channels of leakage of material information (illegal access to physical objects of protection);
- Threats of information leakage through technical channels;
- Threats of unauthorized access to data processed in the local network.

Threats of information leakage through technical channels include:

- Threats of leakage of acoustic (speech) information;
- Threats of leakage of species information;
- Threats of information leakage through the PEMIN channel.

The most significant threats to IS for the bank (methods of causing damage to the subjects of information relations) are:

- Violation of confidentiality (disclosure, leak) of information constituting an official or commercial secret, as well as personal data;

- Violation of the functionality of the components of the information system, information blocking, violation of technological processes, failure to timely solve problems;
- Violation of integrity (distortion, substitution, destruction) of information, software and other resources, as well as falsification (forgery) of documents [S.Vb].

The first chapter of the final qualification paper considers theoretical issues of ensuring IS, classifies threats to protected information, makes a comparative analysis of security methods and means, draws the following author's conclusions - the presence of various types of threats currently requires the construction of an integrated information protection system.

The studies and the obtained conclusions allow us to proceed to the consideration of the material of the second chapter, devoted to the description of existing methods and means of information protection.

Chapter 3

# BASIC METHODS AND MEANS OF PROTECTING INFORMATION ON NETWORKS

## 3.1 Legal and engineering methods and means

Typically, information protection methods include:

- Organizational methods;
- Engineering methods;
- Hardware-software methods;
- Cryptographic methods.

The purpose of introducing the organizational component of the information security (IS) system is:

1. Details of the requirements of the company's IS policy in relation to the conditions of access, circulation and processing of restricted information;

2. Minimization of threats to the IS of limited access, characterized by indicators of their confidentiality, integrity and accessibility, by increasing the reliability of organizational and technological solutions and business processes.

3. Implementation of a systematic approach in decisions, aimed at ensuring the IS of limited access in terms of processing, familiarization and interaction with third-party organizations.

4. Reduction of operational risks associated with restricted information processing technologies.

5. Compliance of the company with the requirements for the IS of limited access, imposed by legislative acts.

To create a private security policy, you need to approve a list of all sensitive data in the company, and prepare a list of employees, who may have access to this data. It is necessary to add a mandatory clause in the employment contract on the prohibition of the disclosure of data, to which the employee gains access by virtue of official duties [MV].

Engineering protection of information aims:

- To secure the building and premises from the penetration of unauthorized entities in order to steal, damage or alter information;
- To prevent damage or complete destruction of information media from the consequences of natural disasters and from the effects of water during fire fighting;
- Block access for attackers to all technical channels through which data leakage may occur.

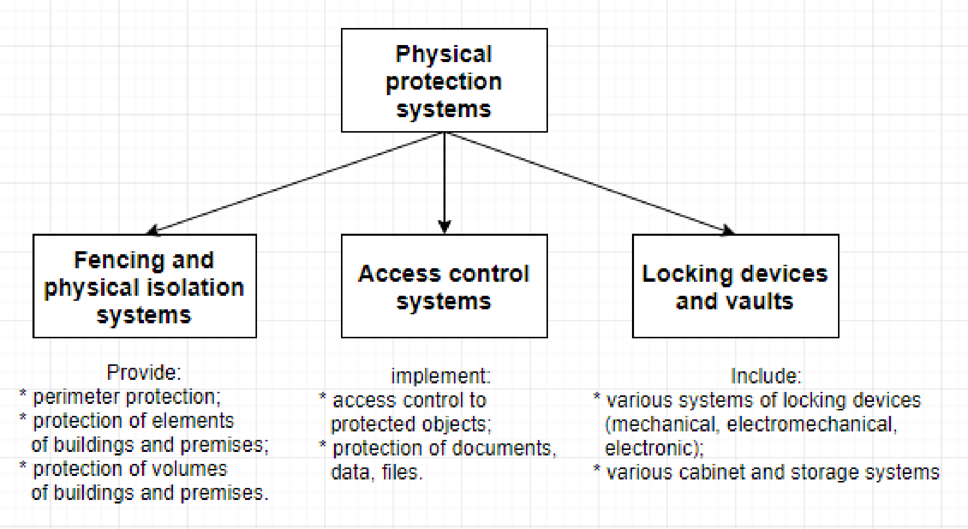

Physical protection systems
Fencing and physical isolation systems
Access control systems
Locking devices and vaults
Provide:
* perimeter protection;
* protection of elements of buildings and premises;
* protection of volumes of buildings and premises.
implement:
* access control to protected objects;
* protection of documents, data, files.
Include:
* various systems of locking devices (mechanical, electromechanical, electronic);
* various cabinet and storage systems

**Figure 3.1:** Physical security systems [N.V]

The composition of the engineering and technical support of IS includes a video surveillance system, access control and management system, as well as security and fire alarm systems. All physical means of protection are based on the interconnected use of various mechanical, electronic or electromechanical devices that are specially designed to create various kinds of obstacles on the possible ways of unauthorized penetration of violators to the system itself or its components. It also includes video surveillance and burglar alarms [N.V].

Hardware and software (technical) protection measures are usually created on the basis of various electronic devices in conjunction with special programs that perform (independently or in conjunction with other similar means) protection functions, such as authentication and identification of each user, access control, recording all system events, data encryption, etc. [Pos], [A.Vb].

Considering all the requirements and principles of IS, all areas of protection and the system itself should include the following:

- Means of delimiting access to information and providing cryptographic protection;
- Means of control and registration of all calls to information system data, their change and use;
- Means of response to external and internal intruders, as well as counteraction to various intelligence mechanisms and methods;
- To prevent illegal access of unauthorized persons to data and information, reliable recognition mechanisms for each user (or individual groups) must be provided [RB]. Various devices can be used for this: keys, magnetic cards, floppy disks, etc.;
- Hardware and software ISs are designed to solve the following set of tasks for protecting confidential information, processed in corporate applications [S.Vb];
- Implementation of secure processing on a single computer of data of various categories of confidentiality with the prevention of theft, disclosure of confidentiality during theft and unauthorized modification of confidential data;
- Implementation of protection of system resources of computers within the enterprise automated system (AS);
- Implementation of a secure connection of computers to a local and external network;
- Implementation of collective access for enterprise employees to the protected resources of the enterprise AS;
- Implementation of effective tools for a security administrator (Workstation of the administrator of the enterprise AS).

Every year, information technology continues to develop rapidly, thereby creating new ways of influencing information. The development of information technology enables enterprises to optimize their work through digital copies of data, which have a number of advantages over physical media: quick access, long-term storage without deterioration of the final information source, preservation of physical space, etc. But in addition to the positive aspects, there is also a negative vector in the application of information systems: the complexity of ensuring IS, the maintenance of information media, backup data acquisition and hiring specialists in the field of maintenance and security of digital information, purchase or development of specific software.

To implement effective management in modern realities, the protection of information is a prerequisite, as it is necessary at all stages of the development of the organization. In this case, we look directly at corporate networks. It is they, who more often than others are exposed to threats, since through them there is a flow of information characterizing the activities of the organization. Stopping this flow of information paralyzes all activities of the organization, which causes serious material losses and loss of image.

Experts note that the main threat to information technology infrastructure is the virus (Trojan, worms), but do not forget that spyware, spam, phishing attacks (a form of Internet fraud aimed at gaining access to confidential information), social engineering. According to Kaspersky Lab JSC, an international company developing solutions for providing information technology - security, we display the following indicators of active virus. Security threats of local area networks are a serious problem for the enterprise, as this means that the attacker entered the organization or recruited one of the employees. Access is obtained from one of the enterprise's computers, that is, it has a direct connection to the local computer system of the company from the inside, which can lead to mass failures, information leakage and its complete loss.

Web threats are one of the most common types of attacks. Its essence lies in the use of malicious URLs for the introduction of malware. Malicious scripts are also used to crack legitimate sites.

## 3.2 Hardware-software and cryptographic methods and means

### 3.2.1 Information encryption

For IS cryptographic tools are also used that support the encryption of secret data stored on HDD or other media. In this case, the key required to decode secret data is stored separately from the data. Typically, it is recorded on an external disposable medium - a Touch Memory key or a USB drive. And if the intruder steals the carrier of secret data, he is not able to decrypt them without having the required key.

Having analysed various approaches to the definition of IS, we can conclude that it has a huge range of tasks that can be divided into two large areas. The first is the satisfaction of information needs, which consists in providing subjects with the information they need. The second - includes the protection of information, which is required to ensure the comprehensiveness, authenticity and efficiency of the information provided, and its security.

In cryptography, experts distinguish two encryption methods. The first method is called the "symmetric encryption method", the essence of which is that the same key is used for encryption and for decryption (for example, DES, IDEA, etc.). The second method experts call “asymmetric encryption”. Here one key, it is called open, is used for encryption, and for the purpose of decryption another key is used, called private (for example, El-Gamal, Elliptic curves) [G.G].

Having studied the methods of cryptography, it is necessary to consider specific examples. According to the researchers, today it is very difficult to evaluate the reliability of the transmitted data, since almost all data cryptography systems are implemented through closed modules of foreign origin. But we understand that encryption systems of foreign origin are also used in the public sector, and this is completely undesirable and, in many cases, even prohibited by law.

As mentioned above, the need for encryption of personal data is emphasized at the state level. Importance of providing free access to encryption means for “electronic interaction with state authorities and local governments”. The government will have to take legislative measures that would exclude "the use of equipment that allows third parties to interfere with the operation of cryptographic protocols, when transmitting data using a public communication network."

Encryption is actively used not only in management, but also in other areas of activity. Let’s look at some examples.

Data encryption according to the end to end model, when data is transferred from one wireless device to another and is available for reading, viewing, listening only to the sender and recipient, has been used by the Telegram messenger for several years now. In early April 2016, the WhatsApp messenger introduced this technology. On April 19, 2016, another popular messaging service, Viber, announced the start of data encryption.

Google and Microsoft, together with the largest email providers in March 2016, began developing an e-mail service that cannot be “tapped”: a group of independent researchers together with five companies (Google, Microsoft, Yahoo, Comcast and LinkedIn) proposed standardizing a new extension for the protocol SMTP Cryptographic algorithms and protocols are widely used to ensure the IS of modern information and telecommunication systems. At the same time, some types of cryptosystems are the basis of new information technologies, for example, those technologies that necessarily require solving the problems of authenticating the message source, giving legal force to electronic messages, and ensuring anonymity of users. Modern cryptography is a developed branch of modern applied mathematics and applied technical discipline. It offers a wide arsenal of tools for solving various tasks of ensuring IS, but practical informatics raises new urgent issues, stimulating new scientific and technical research and obtaining new results.

Next, we consider some relatively new cryptography issues and the results obtained related to their solution, as well as issues of expanding the functionality of electronic digital signature (EDS) standards, formal proof of the stability of EDS algorithms based on the complexity of the discrete logarithm problem (DLP), increasing the level of security of crypto currencies, increasing the strength, when encrypting messages using small keys, ensuring the security of secret information with the so-called "coercive" a such, in the model of which it is assumed that the attacker is provided with an encryption key.

### 3.2.2 Extending the functionality of electronic digital signature standards

The issue of expanding the functionality of official EDS standards is related to the fact that most of the standards specify an individual digital signature scheme, while practice requires other types of EDS protocols, for example, collective, group and blind signing. Adopting new standards is a long-term and resource-intensive process. Instead of adopting independent standards for all popular types of EDS protocols, an approach is considered in [1-4] that consists in using a standardized scheme of an individual EDS to build the following types of protocols on its basis: 1) collective, 2) blind and 3) blind collective signature. In this approach, it is proposed to develop such protocols of the latter type, for which a reduction proof of resistance can be given (if the protocol is not stable, then the basic scheme on which the protocol is based is not stable) and for their practical implementation it is not necessary to introduce any or changes to an existing public key infrastructure. It was shown that this approach is applicable to the standards GOST R.34.10-2012, the standards of Belarus STB 1176.2-99, Ukraine DSTU 4145-2002 and Germany ECGDSA. It is also of interest to implement a group signing protocol with masking of public keys of signatories, proposed in [M.Ac], based on these standards, but this issue is not reflected in well-known publications.

### 3.2.3 Formal proof of persistence of electronic digital signature standards

Formal proof of the strength of public key cryptosystems provides the most complete recognition of the security of their use. In the case of EDS schemes based on the computational complexity of the DLP, the most well-known method of formal proof of durability proposed in [GS] is applicable to crypto circuits in which a randomization parameter is first generated in the signature generation procedure (also called a fixer), and then the first element is calculated EDS in the form of a hash function value, which is calculated from a message with a latch attached to it. These schemes include EDS protocol EDS Shnorr. However, for the most well-known standards, such evidence does not apply.

Another approach to the formal proof of the durability of EDS circuits based on DLP is the approach proposed in [10], which consists in deriving the considered circuit from a protocol with zero disclosure, for which it is formally proved that the complexity of forging the correct answer to a random request from a tester has one the order with the complexity of the DLP underlying the protocol. The latter approach requires the construction of new three-pass protocols with zero disclosure with an open key, which has the same form as the public key used in the EDS scheme. To solve this problem, an extension of the types of protocols with zero disclosure is proposed, based on the interpretation of the term “zero disclosure”, based on statistical equivalence with a set of random parameters, generated during the simulation procedure authentication, performed by a potential attacker. Using this interpretation of the physical meaning of protocols with zero disclosure, it becomes possible to build significantly more diverse protocols of the type under consideration, including protocols that can be converted into digital signature schemes specified by GOST R.34.10-2012, STB 1176.2-99, DSTU 4145-2002, DSA, ECDSA and ECGDSA [A.Aa]. Moreover, for such protocols with zero disclosure, a formal reduction proof of the resistance to falsification of a response to a random request can be given and the proof is based on the standard assumption of the stability of the used hash function (the same assumption underlies the generally accepted method of formal proof of the stability of the Schnorr EDS scheme, considered in detail in [GS], [A.Aa]). Since in the EDS scheme, constructed by its derivation from the protocol with zero disclosure (i.e., by converting the latter to the EDS scheme), the value of one of the signature elements is actually response to a random request, calculated depending on the fixator and the value of the document. Signature falsification means faking the correct answer in a zero-disclosure protocol, i.e. Computational complexity of signature falsification is of the same order as the complexity of DLPs, used to construct the EDS scheme.

### 3.2.4 Improving the security of public-key cryptosystems

For the practical use of cryptographic algorithms and protocols (cryptographic schemes), various aspects of their implementation are important: stability, computational complexity of the procedures used, hardware and software implementation, etc. Moreover, improving the parameters of cryptographic schemes by modifying them or constructing new algorithms and protocols, makes sense only if when this is carried out as part of the requirement to ensure a given level of durability. The concept of durability characterizes the most important property of cryptographic schemes to withstand all kinds of attacks and is measured by the number of certain operations that need to be performed for the case of applying the most effective known attack in order to crack the cryptographic scheme. The fundamental point for assessing the durability is the question of the best-known cryptographic cracking algorithm. If it is possible to formally prove its durability for a crypto scheme, then this question carries over to the computationally difficult task, used to construct the crypto scheme. Usually, for the construction of crypto currencies, the long-known and well-studied computationally difficult problems are used as basic difficult problems, for the solution of which breakthrough solutions (having polynomial complexity) are unlikely to occur, which would mean breaking a whole class of crypto currencies, i.e. all those crypto currencies based on this task. The fundamental problem of assessing the strength of crypto currencies is that it is difficult to prove that breakthrough solutions of the basic difficult problem do not exist or at least in the near future, which would give a solid justification for assessing the strength of the crypto circuit as the computational complexity of the best known algorithms for this problem.

When it is said that the crypto scheme is stable in the sense of the security of its use for solving IS problems, it is clearly believed that the value of the resistance exceeds a certain set sufficiently large value, for example, 280 (80-bit 128 192 resistance), 2128 (128- Bit Strength) or 2192 operations (192 Bit Strength). At the same time, it is implicitly assumed that the probability of breakthrough solutions in the foreseeable future for the basic difficult problem (for provably stable two-key cryptographic schemes) or breakthrough attacks (in the general case) is negligible. The latter provision is also fundamentally important when it comes to the security of using crypto currencies for solving various practical problems. The concept of durability reflects only one of the two sides of the concept of security of crypto currencies. The second side is the likelihood that in the foreseeable future no breakthrough results will be obtained on the development of algorithms for solving difficult problems used. A quantitative safety assessment should include quantitative estimates of resistance and specified probability, for example, a quantitative safety measure can be defined as the ratio of resistance to probability. Such a formula clearly shows that an increase in the security provided by crypto currencies can be achieved both by increasing the size of the parameters of the crypto circuit, leading to an increase in the value of resistance, and by reducing the value of the specified probability.

This interpretation of the concept of security is the basis of one of the areas of research in cryptography, related to the construction of crypto currencies, the breaking of which requires the simultaneous solution of two independent difficult computational problems. When constructing such crypto currencies, it is assumed that the computational complexity of each of the tasks used has a value, equal to or superior to a given level of stability and the achievement of an increase in the security value is achieved by multiplying small probabilities, related to the events of the appearance of breakthrough solutions of the two used difficult problems. In this direction, the combination of the factorization problem (FP) of integers of a special type and DLP in a simple module is most often used. Initially, EDS protocols of this type were developed [EN], [A.Ab], [A.E], [V.Aa]. The latest results of this area of research, relate to the development of a general approach to building crypto currencies, based on the difficulty of FP and DLP in a simple module [oEC], [KN]. The general approach allows us to develop algorithms and protocols for open key agreement, open encryption, commutative encryption, digital signature and other. The essence of the approach is to use DLP in a difficult decomposable module and based on the fact that the sub-exponential solution of the latter problem requires solving the FP composite module and solving DLP by a module, equal to each of the simple divisors of the module. Moreover, for the case of the implementation of EDS protocols, an increase in productivity and a decrease in the signature size are achieved at a given level of durability.

### 3.2.5 Choice of information protection system

For the effective selection or construction of an information protection system, as well as maintaining its functioning, certain conditions should be met:

- Identify and consider all possible threats to information requiring protection;
- Clearly articulate the security policy, not only of the computing system, but also of the organization as a whole;
- To work out the complexity of the protection structure, containing all the necessary and compatible with each other information protection mechanisms;
- Monitor the system, conducting systematic checks of its functioning.

Only compliance with the above conditions will allow us to provide a certain level of information security, which is so necessary for us in the age of information technology. The possibility of using the procedures for the formation and verification of electronic digital signatures, which are specified by a number of official electronic digital signature standards in blind and collective signature protocols, shows that the latter can find wider application than their original purpose. This shows that the EDS scheme used in them is preferable to the EDS scheme of the American DSA and ECDSA standards, for which the specified extension of functionality cannot be implemented.

The proposed approach to the formal proof of the resilience of EDS standards is a significant contribution to the justification of their resilience and puts them on a par with provably robust EDS algorithms.

The considered concept of the implementation of the OS procedure as a cryptographic transformation procedure that is computationally indistinguishable from probabilistic encryption is of interest for constructing OS algorithms, using a public key, which, apparently, will solve the problem of ensuring the high speed of such algorithms and expand their potential applications.

The classification of cryptographic systems is based on the following three characteristics:

1) The number of keys used;

2) Type of operations for converting plaintext to encrypted;

3) The method of processing plaintext.

1) By the number of keys used.

Distinguish:

- Symmetric cryptosystems;
- Asymmetric cryptosystems.

If the sender and the recipient use the same key, the encryption system is called symmetric, a system with one key, a system with a secret key, a traditional encryption scheme. (For example, DES, CAST, RC5, IDEA, Blowfish, classic ciphers); If the sender and receiver use different keys, the system is called asymmetric, a system with two keys, a public key encryption scheme. (RSA, El Gamal).

2) By type of operations for converting plaintext to encrypted.

- Wildcard ciphers - Encryption is based on replacing each element of the plaintext (bits, letters, groups of bits or letters) with another element. (Caesar, Playfayer, Hill);
- Permutation ciphers - encryption is based on changing the sequence of clear text elements. (Ladder, rearrangement of columns);
- Production ciphers - encryption is based on a combination of several replacement and permutation operations. Production ciphers are used in most real-life modern encryption systems (DES).

3) According to the method of processing plaintext.

- Block ciphers - block ciphers are called ciphers in which the logical unit of encryption is a block of plaintext, after converting which a block of cipher text of the same length is obtained. For example: DES, Feistel cipher.
- Stream ciphers - mean encryption of all elements of the plaintext sequentially, one after another (bit by bit, byte by byte).

Examples of classic stream ciphers are the Vigenere ciphers (with automatic key selection) and Vernam cipher. Block ciphers are much better studied. It is believed that they have a wider scope than in-line. Most network applications that use the traditional encryption scheme use block ciphers.

Symmetric cryptosystems (also symmetric encryption, symmetric ciphers, symmetric key algorithm) - a method of encryption, in which the same cryptographic key is used for encryption and decryption. Prior to the invention of the asymmetric encryption scheme, the only existing method was symmetric encryption. The algorithm key must be kept secret by both parties. The encryption algorithm is chosen by the parties before starting the messaging.

A public key cryptographic system (or asymmetric encryption, asymmetric cipher) is an encryption and/or electronic signature (ES) system in which the public key is transmitted over an open (that is unprotected, observable) channel and is used to verify ES and for encryption messages. The private key [M.Aa] is used to generate the electronic signature and to decrypt the message. Public key cryptographic systems are currently widely used in various network protocols, in particular, in the TLS protocols and its predecessor SSL (underlying HTTPS), in SSH. Also used in PGP, S/MIME. The scheme was proposed by Taher Elgamal in 1984. Elgamal developed one of the variants of the Diffie-Hellman algorithm. He improved the Diffie-Hellman system and obtained two algorithms that were used for encryption and for authentication. Unlike RSA, the Elgamal algorithm was not patented and, therefore, became a cheaper alternative, since it did not require payment of license fees. It is believed that the algorithm is subject to the Diffie-Hellman patent.

The safety of the Elgamal scheme is due to the complexity of computing discrete logarithms in a finite field. There are a large number of algorithms based on the Elgamal scheme: these are DSA, ECDSA, KCDSA, Schnorr algorithms.

The technology of applying the EDS system assumes the presence of a network of subscribers, sending each other signed electronic documents. A key pair is generated for each subscriber: secret and public. The secret key is kept secret by the subscriber and is used by him to form the digital signature. The public key is known to all other users and is intended for electronic signature verification by the recipient of a signed electronic document. In other words, a public key is a necessary tool to verify the authenticity of an electronic document and the author of a signature. The public key does not allow to calculate the secret key.

RSA (an abbreviation for the names Rivest, Shamir, and Adleman) is a public-key cryptographic algorithm, based on the computational complexity of the large integer factorization problem.

IDEA (International Data Encryption Algorithm) is a symmetric block data encryption algorithm patented by Ascom, a Swiss company. Known, for being used in the PGP encryption software package. In November 2000, IDEA was nominated as a candidate for the NESSIE project within the framework of the European Commission's IST (Information Social Technologies) program.

The RSA cryptosystem was the first system, suitable for both encryption and digital signature. The algorithm is used in a large number of cryptographic applications, including PGP, S/MIME, TLS/SSL, IPSEC/IKE and others. The algorithm has an encryption key length of 256 bits, encrypts information in blocks of 64 bits (such algorithms are called block), which are then divided into two 32-bit subunits (N1 and N2). Subunit N1 is processed in a certain way, after which its value is added to the value of subunit N2 (addition is performed modulo 2, that is the logical operation XOR is used - “exclusive or”) and then the subunits are swapped. This conversion is performed a certain number of times (rounds): 16 or 32, depending on the operating mode of the algorithm.

Unlike the algorithm, which has remained secret for a long time, the American AES encryption standard, designed to replace DES, was selected at an open competition, where all interested organizations and individuals could study and comment on candidate algorithms.

Some asymmetric algorithms are used to create a digital signature (DS). In this case, the DS is a data block, created using a separate secret key. At the same time, thanks to the public key, it is verified that the cipher was created using this secret key. The DS creation algorithm supports the inability to create a signature without a secret key, which, as a result of the verification, turns out to be correct. DSs are used to confirm that a message has been transmitted accurately from a given sender (in the format that only the sender has a secret key). The DS is also used to indicate the time stamp on the papers: the party we can trust signs with the time stamp, using a secret key and, as a result, guarantees that the document was already created at the time, indicated in the time stamp. DSs are often used for certificates (or certify) that a document refers to a specific person. And this is done like this: the public key and the data, on whose it is signed by the trusting party. And we are able to trust the signing party within the framework of the fact that its key is confirmed by the 3rd party. The result is a confidence "pyramid". Of course, a separate key becomes the root of the hierarchy (i.e., we trust it not because it was signed by someone, but simply, because it must be trusted from the beginning). In the centralized structure there are several network roots keys (for example, having the authority of a state company, otherwise called certification centres). In a shared infrastructure, there is no obligation to have universal root keys and all parties can trust the set of root keys (their key or keys signed by that party). This approach is referred to as a trust network and is used, for example, in PGP.

The document DS is usually implemented as follows: a selective digest is created from the document and data about who put the signature, time stamp, etc. is added to it. The resulting string is subsequently encrypted with the sender's secret key, using a specific algorithm. The resulting encrypted character set also becomes a signature. Also, the sender's public key is usually given to it. The recipient decides for himself whether he trusts that the sender's public key, i.e. who should belong to (using the trust network or the initial opinion) and then opens the signature with the access key. If the signature was opened correctly and its contents correspond to the document, then the message becomes confirmed. Some of the methods for creating and checking DSs are now available. The RSA algorithm is considered the most popular.

Crypto hash functions are used to create a message digest during DS development. Hash functions show a message that has a specific hash parameter, so that the entire set of available messages is divided in balance by the set of hash parameters. At the same time, the crypto hash function creates this in such a way that it is almost impossible to fit the document to the prescribed hash tag. Crypto hash functions often produce strings of 128 bits or more in length. This number is clearly greater than the sum of messages that may even exist in the world. Part of the great crypto hash functions in the public domain. The most famous have MD5 and SHA.

Random number crypto generators display a random number, used in crypto applications, for example, to create keys. Often, such generators, which are included by default in programming languages and environments, do not meet the needs of cryptography (they are implemented to obtain a statistically chaotic separation. Crypto-analytics are able to know in advance the behaviour of such random generators).

In the best case, random numbers should be based on a specific physical source of random data that cannot be foreseen. Such sources include noisy semiconductors, small bits of digital sound, the intervals between device stops or keystrokes. Noise, received from a physical source, is tested by a crypto hash function so that each bit depends on another bit. Often huge pools (1000 bits) are used to save random data and each bit of the pool is independent of the other bit of the noise data and the other bit of the pool, using a crypto-reliable method.

If there is no physical noise source, pseudo-random numbers can be used. But this approach is undesirable, but sometimes is implemented in general-purpose PCs. It is always optimal to get some kind of ambient noise, say from a delay in devices, the frequency of resource use, network statistics, keyboard keystrokes, or something else. The task is to obtain data that is implicit to an outside observer. To implement this, a random pool must include up to 128 bits of total entropy.

Crypto-random number generators often use a large pool with random data. Bits are created by fetching from the pool with an accessible run through a crypto hash function to close the entire contents of the pool from an outside observer. When the next portion of bits is needed, the pool is rearranged using an encryption method with a random key (it is often taken from the passive part of the pool). So, any bit in the pool is dependent on another. The ambient noise needs to be added to the pool before the mixing operation, in order to make the prediction of new pool values even more difficult.

But even regardless of the fact that with the right construction, a crypto-reliable random number generator is quite simple to create the described moment is often forgotten. As a result, it is important to emphasize the relevance of the random number crypto generator: if it is incorrectly made, it becomes an easily vulnerable part of the system.

## 3.3 Comparative analysis of methods and means of protecting information in computer networks

The classification of information protection methods is shown in figure 3.2.

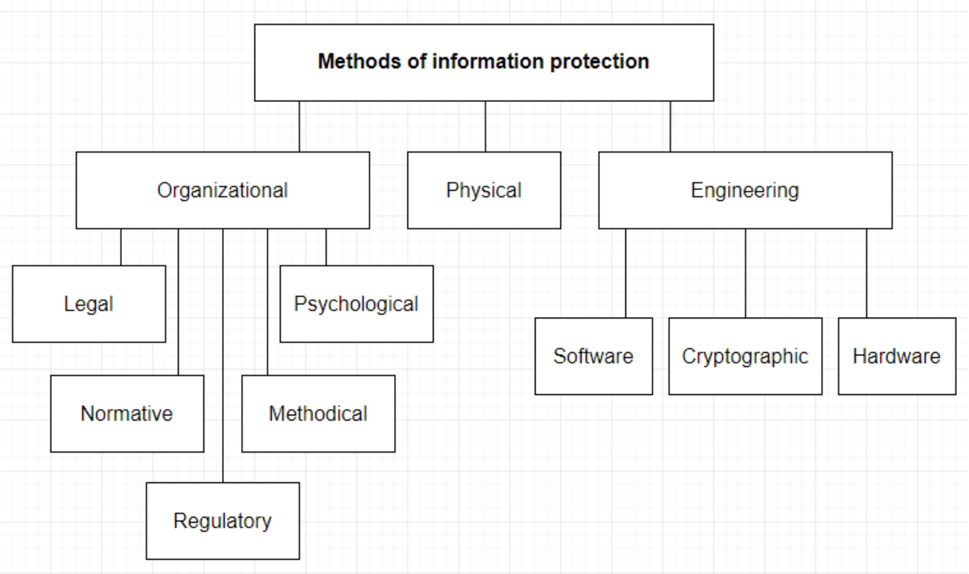


**Figure 3.2:** Information security methods [M.Aa]

Consider the main content of the presented methods of information protection, which form the basis of protection mechanisms (figure 3.3).

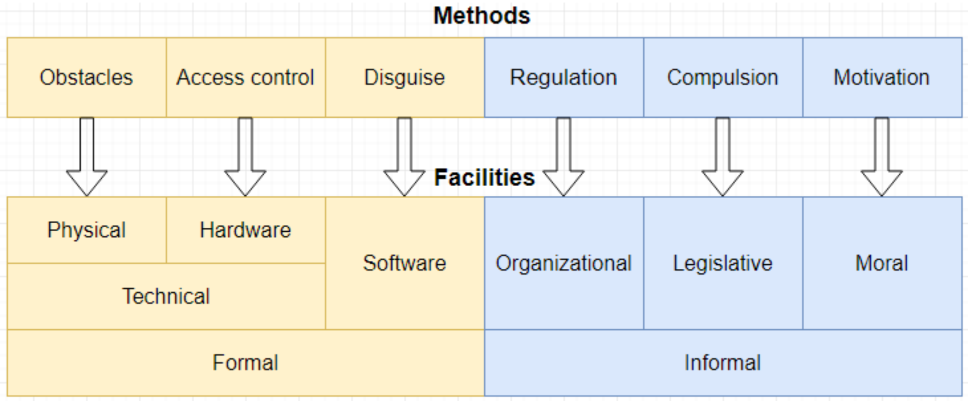


**Figure 3.3:** Methods and means of ensuring information security [M.Aa]

Methods for ensuring the information security in IP:

- An obstacle;
- Access control;
- Encryption mechanisms;
- Countering malware attacks;
- Regulation;
- Coercion;
- Motivation.

Today, there are such ways of protecting confidential computer information from unauthorized access by third parties as (figure 3.4):

- Strong authentication systems (AS);
- Prevention of misuse of information resources;
- Audit of the actions of network users;
- Archiving confidential correspondence;
- Encryption of confidential data.

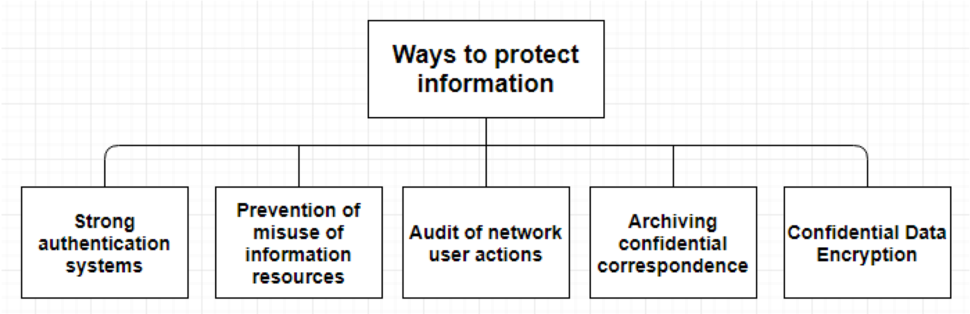

Ways to protect information
Strong authentication systems
Prevention of misuse of information resources
Audit of network user actions
Archiving confidential correspondence
Confidential Data Encryption

**Figure 3.4:** Methods for protecting confidential computer information from unauthorized access [M.Aa]

Software and technical methods - this is precisely the practical and very extensive protection base that is constantly being revised and improved by specialists in the field of IT security. It includes various measures, aimed at preserving data, both in the event of failure of storage media and in the case of a targeted attack on the database by attackers. It also provides methods of protection against illegal data interception, while listening to conversations, etc. Many of us know some methods, for example, passwords and accounts (which is the most vulnerable place for hacking), encryption, auditing, antivirus software, etc.

Very reliable and popular means of protecting information from interception include key carriers that are created to store sensitive information. Usually, a USB token (a complex device resembling an external flash card) is used, which allows the employee to access the computer and the Internet, and also provides access to a system, where all financial transactions are carried out.

In the process of development and construction of systems for protection against data loss in a nuclear power plant, it is necessary to adhere to some system principles that are an application of the basic principles for the development of complex systems, taking into account the specifics of the processed tasks for implementing data protection in a nuclear power plant:

- A systematic approach to creating protected automated system (AS);
- Parallel development of IS system and AS;
- Use of a hierarchical control system for data protection functions in AS;
- Multilevel structure of IS tools;

- The possibility of further modification of the IS system complex;
- Block architecture of a secure automated system;
- Convenient user interface of the AS itself.

Protection of information resources should be implemented along the entire chain of input, transmission, processing, storage and delivery of data. The IS system complex itself should not have weak points at any stage of the life cycle, or in any of its element or mode of operation. The complexity of such a data protection system requires the right combination of various means; software in various ways interacts in hardware, while various organizational measures are also envisaged. In this case, not all protection mechanisms can be provided only by IS system.

The control subsystem is a functional subsystem of the IS system unauthorized access inside the AS, which supports its control functions and it works due to the combination of methods and tools, previously provided in the AS for the management of all available IS system unauthorized access. The criterion for the optimal control of the IS system unauthorized access in the AS should have a comprehensive character, which leads to multi criteria tasks of the optimal control [A.Ab] of the protection mechanisms. This is due to the conflicting nature of the use of AS resources by processing mechanisms and information protection mechanisms.

Under these conditions, the solution of the problems of organizing the optimal management of IS system unauthorized access in the AS is directly related to the justification of the possibilities, for using the resources of the AS and, as a consequence, the need to justify the requirements for the characteristics of the IS system. Currently, the content of the requirements for IS system unauthorized access and the procedure for their assignment is determined by the current documents of the FSTEC (Federal Service for Technical and Export Control), which specify only high-quality requirements for IS system on the composition of their protective functions.

This makes it necessary to supplement the existing qualitative requirements for the protection of information with quantitative ones, which, in turn, leads to the need to move from the existing organizational practice of managing the IS system unauthorized access to organizational and technological. Such a transition can be provided by means of supporting managerial decision-making on the basis of a comprehensive assessment of the quality of functioning of the IS system unauthorized access in accordance with mathematical models of the process of its functioning [V.Aa]. Such funds are an obligatory component of IS system complexes. An obstacle refers to methods of physically blocking the road for an unauthorized user to information that must be protected.

Usually, an organizational means provides for the regulation of any production activity within the framework of IP as well as all the relationships of performers at such a level that any leak or unauthorized disclosure of confidential information becomes simply impossible or is very difficult, due to the complex of measures taken. This set of measures is usually implemented by a separate IS group and always is under the control of senior management.

Organizational measures to ensure IS are the core of all measures to build an IS system. The effectiveness of the information protection system as a whole depends on how fully and efficiently the management of the enterprise has built organizational work to protect information, since the correct formulation of the task of ensuring measures to protect information and the competent distribution of responsibilities between performers is the foundation for building any system.

The place and role of organizational measures in the general system of methods used to protect the confidential information of an enterprise is determined by the importance of top management, making timely and balanced decisions based on the current situation with information protection, including as a result of analysis of the company's methods and means of ensuring IS, using current package of legislative acts. The competent implementation of the IS policy of a modern industrial enterprise involves the application of an integrated approach.

The main integrated approach is organizational methods, among which the most important is the development of IS policies. Such a document means a description of a set of rules, procedures, methods and ways to ensure IS in organization.

As a result of the second chapter of the final qualification work, it is possible to draw the author's conclusions that the methods and means of information protection should be applied comprehensively, which allows us to go to the third chapter of the work.

Chapter 4

# IDENTIFICATION OF THE MOST RELEVANT THREATS AND SELECTION OF REMEDIES

## 4.1 Main threats and vulnerabilities of industrial information systems

Information technologies (IT) and information systems (IS) are currently used in all spheres of the state's life support. According to their intended purpose, IS are divided into two classes:

- Information-organizational system (IOS);
- Information-management system (IMS).

IMS are intended for the management of technical facilities, based on the analysis of the characteristics of the processes occurring in them, the system generates control actions. Industrial control system (ICS) at production is a type of ICS that requires operators to perform certain functions of managing labour costs, including technical means that ensure the replacement of the physical and mental labour of a person with the work of machines for collecting, processing and outputting information [M.Aa].

The main functional purpose of ICS is the creation of conditions for work and business, automation of people's work. Process control systems have a multi-level structure [AD]:

- The level of operator (dispatch) control (upper level);
- The automatic control level (middle level);
- The level of actuators, as well as input, output of data (lower level) [AD].

The safety of ICSs consists in the formation and maintenance of such conditions for the functioning of the system, in which the quality of the process control does not lead to unacceptable damage to the technological complex itself, the environment or human resources. The operating conditions of ICS should ensure the security of the system from threats to violation of the confidentiality of information circulating at the upper level, threats to its integrity at the middle and lower levels, as well as against threats to the violation of the availability of information services for personnel.

It was previously believed that automatic process control systems themselves are difficult to crack systems due to the use of specific equipment and software, but with the advent of modern technology, everything has changed. The development of modern technologies has led to the fact that in modern management systems, to reduce the costs of development and implementation, widespread operating systems, network equipment and network protocols that have flaws in the form of vulnerabilities, began to be used.

Automated process control systems have become inherent in almost all the vulnerabilities of modern information systems. More than a hundred vulnerabilities were discovered in the components, used to control technological processes at industrial facilities in 2017 [G.G]. Using publicly available search engines, potential attackers can remotely access ICS components, including 4.5 thousand devices that ensure the operation of energy facilities around the world. Almost half of the vulnerabilities identified in 2017 are high, with the largest number of vulnerabilities found in the products of the most famous manufacturers. A study was carried out on the availability of open ports of ICS components that are accessible via the Internet. The study showed that at one critical facility there can be up to 50 thousand open ports of ICS components, which allow an attacker to attack the system and disrupt the availability of the ICS component [G.G].

The largest number of vulnerabilities was found in SCADA systems (43%), in specialized network devices (28%), in the software for dispatch and operator control systems of automated process control systems (19%), in PLC (17%). Moreover, 47% of the listed vulnerabilities are high, and only 14% of the vulnerabilities declared by specialists are eliminated within three months after detection [G.G], [S.Vb]. It is noted that a third of the used automated process control systems, connected to the business circuit are almost not protected from external sources of threats [S.Vb].

Currently, many industrial enterprises include ICS segments as part of corporate information systems (CIS). Of course, from a safety point of view, segregation of process control systems from the rest of the CIS is desirable. However, it is known that the industrial process control network can be part of the enterprise CIS. The fact is that the highest level of automation maturity is characterized by sophisticated production management processes, the ability of ICSs quickly to adapt to changes in business processes, the integrated use of new information technologies. In order to ensure efficient production management by increasing efficiency, that is, reducing the length of the management cycle, systems such as Enterprise Resource Planning (ERP) and Manufacturing Executive System (MES) have been developed [M.Ac], [GS].

At modern industrial enterprises, ERP and MES enterprise resource accounting systems are being introduced or are already being used. The use of these systems makes it possible to automate the accounting of used resources, time and products. In addition, using the above-mentioned systems, production goals are set (for example, for each workshop of an industrial enterprise its own production plan is set within a certain time frame). ERP and MES systems at industrial enterprises have a direct connection with the upper level of process control systems and other segments of corporate information systems (CIS) [154].

The problem of ensuring information security of automated process control systems is one of the urgent today. The solution to this problem is impossible without developing a model of the essential environment, in which the information security system of ICS operates, that is, without researching and building a model of information base violation threats. The success of the creation of information security system of ICS largely depends on the adequacy of the model of the significant environment; to those destabilizing factors affect the functioning of the protection object – ICS.

Consider the option of connecting the automatic process control system to the enterprise information system, which requires more attention from information security specialists. In figure 4.1 presents a generalized architecture of the CIS segment with ICS.

On the perimeter of the corporate information systems segment with ICS, an Internet router and a firewall are used, which are reserved in case of a failure. Behind the cluster of firewalls there is a demilitarized zone with public servers (web, e-mail, etc.). The external subnet of the segment includes workstations and servers of the business unit of an industrial enterprise, whose employees do not have direct access to the information resources of process control systems. An external subnet may include local network segments, for example, design, technology departments, planning, software development, or others. The internal subnet, which includes workstations and process control servers, is separated from the external subnet by an additional cluster of firewalls.

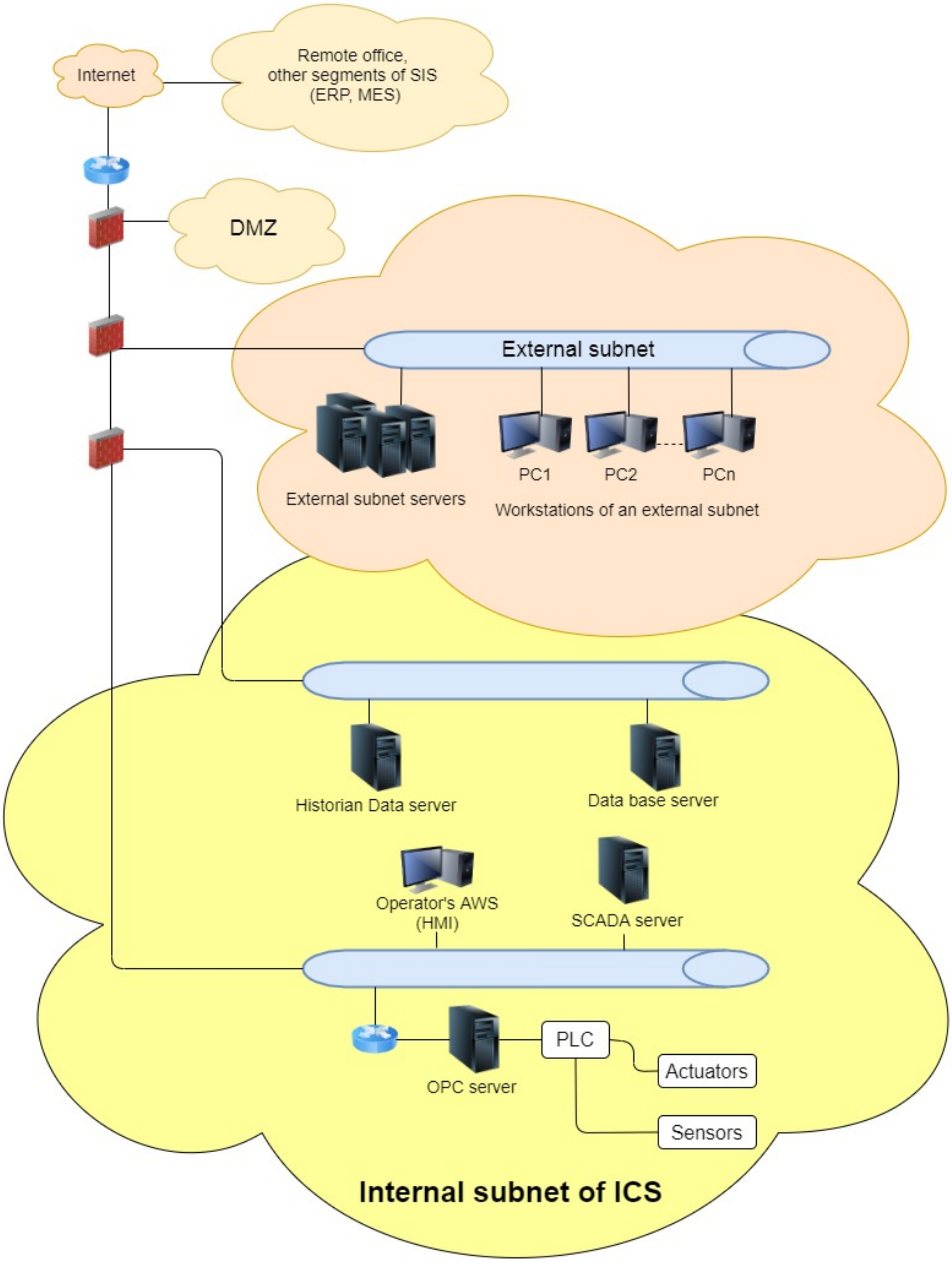


**Figure 4.1:** The generalized architecture of the corporate information system (CIS) segment with industrial control system (ICS) [A.Aa]

Servers, that process limited access information, designed to ensure the production process in process control systems are located in the shielded subnet of the CIS segment (Historian Data Server and Database Server) and in the internal subnet (SCADA, OPC).

At the upper level of the ICS are computer facilities:

- Database server;
- SCADA server;
- Automated workstations of operators (dispatchers).

At the upper level, the data coming from the lower level is processed. Data processing implies: structuring, archiving and subsequent storage, providing data to operators and dispatchers for working with them using the human-machine interface (HMI - Human-Machine Interface). At the upper level of ICS, in addition to processing data from the lower level, control functions are implemented.

At the middle level (automatic control level) are automation tools such as programmable logic controllers (PLC).

At the lower level are actuators and sensors. Servo drives, electric motors, pumps and mechanisms that are used in various types of production can act as actuators. To obtain data on the flow of technological processes, various sensors and other information retrieval devices are used. The composition, the number of ICS levels and the performed target functions depend on the purpose of the system and are determined by the specifics of production processes.

The main vulnerabilities of modern ICS are experts [AD], [G.G]:

- Absence or weak protection against unauthorized access to automated control systems (passwords, personal identifiers);
- Undeclared capabilities of SCADA systems (supervisory control systems and data collection);
- Use of wireless communications (insecure wireless connections);
- Lack of clear boundaries between different network segments (for example, between corporate and industrial);
- Use of remote-control methods (possibly via insecure communication channels); Rejection of minimal security measures (since, often for the sake of convenience

and productivity, companies refuse to install not only, for example, anti-virus, but even password protection of critical assets);

- Untimely or incorrect software updates;
- Rejection of minimal security measures (since, often for the sake of convenience and productivity, companies refuse to install not only, for example, anti-virus, but even password protection of critical assets);
- Distribution of Windows as the main operating system for workstations and even for servers;
- Web-technologies, used at the top level of ICS (if those are used, for example, in HMI).

The following is a list of the main threats to information security of automated process control systems noted in real incidents [S.Vb]:

- Attacks on control nodes;
- Attacks on SCADA systems;
- Attacks on programmable logic controllers (PLC) using vulnerabilities of the PLC itself (default password, unauthorized access to proprietary software, remote password change, etc.);
- Attacks using protocol vulnerabilities, used in the enterprise information management system (OPC - buffer overflow, TCP/IP protocol vulnerabilities);
- Attacks on databases of industrial systems (unauthorized access, SQL injections).

The implementation of the above threats can lead to irreversible consequences, such as:

- Failure of industrial equipment (equipment malfunctioning, control system failure, etc.);
- Technological disasters (industrial accidents);
- Human casualties (among employees and civilians);
- Environmental disasters (environmental pollution);
- Material and financial losses for the enterprise or the state.

Before constructing the information security system of automated process control systems, it is necessary to determine from what, in fact, it is necessary to protect information, that is, to build a threat model for this specific protection object. The threat model should include a list of potential threats, taking into account the adopted security policy, which may affect the information during its processing. Thus, a fundamental feature of the problem of information protection in ICSs is the requirement to fully identify possible threats to the information circulating in the infrastructure of the protected object, taking into account specific vulnerabilities. Intentional threats are the main factor that must be considered when designing an information security system for ICS. The paper proposes the creation of a threat model based on the classification scheme of threats given in [11]. Threat modelling is essentially the only method of a sufficiently complete study of potentially possible destructive effects on the information environment of ICSs. When modelling intentional threats, it is necessary to strive for a complete description of all possible ways of their penetration, taking into account the many possible mechanisms for their implementation.

All information systems are designed on the same principles (infrastructure, network protocols). Therefore, they have almost the same reasons for the success of deliberate threats: incorrectly designed access control policies, lack of barriers to attack, incorrect communication equipment and security settings, software vulnerabilities providing. The paper proposes to consider each threat of violation of data base of ICS as a complex sequence of actions and events that occur during the operation of the protection object, leading it to a subset of situations, in which unauthorized access or destructive changes in the information environment become possible. When using cryptographic protocols in the attacked ICS, the adversary, based on cryptanalysis methods and some assumptions, carries out an attack on the cryptosystem. The set of such attacks is constantly expanding due to the development of theoretical methods of cryptanalysis and the capabilities of technology. In general, attacks on the cryptosystem are successful only with oversights, made during the implementation of the cryptosystem.

Scanning and detecting open ports can allow an attacker to identify active services and exploit their vulnerabilities. By gaining access to the information environment of the CIS segment with automated process control systems, an attacker may try to filter identification and authentication information. As a result of its interception, it becomes possible to extract passwords from the general stream. As a result of enumeration of vulnerabilities, it is possible to obtain input to a host. The access, obtained as a result of these actions, can have a different level. An attacker can gain access as a user with insignificant rights, in which case an attempt will be made to collect “garbage” on the hard disk and RAM. The result may be obtaining authentication information that allows you to organize a higher level of access, at which an attacker can inject mobile malicious code that allows you to collect or destroy the required information, unauthorized access to the required information, or even change the protection (settings) databases, which will allow you to create credentials records of non-existent users with access rights. When an attacker can modify the transmitted data (text or executable code), he can affect the integrity of the executable code or introduce malicious software (MSW), which will allow him, after transmitting the packet to the server, to act on the user authentication program in the database and receive high rights.

The developed threat models in the ICS reflect the orientation of the carrier propagation vector, when the threat is implemented on many components of the infrastructure of the protection object, the location of the information source (SCADA, OPC, PLC, and operator's workstation), the sequence of the attack and the vulnerabilities used, as well as the potential attacker.

Target points of the ICS infrastructure that attack vectors are aimed at: the operator's and dispatcher's automated workstation (hereinafter referred to as the operator's workstation), SCADA servers, and programmable logic controllers (PLCs). Including, OPC servers are often used in modern process control systems.

In this paper, to simulate threats to information security breaches of ICS, we use EPC graphical notations (Event-Driven Process Chain), the key elements, of which are Events and Functions, connected by logical operations [A.Aa]. Logical relationships are used to branch the process, described by the symbols "AND" (), "including OR" () and "exclusive OR" (XOR). EPC models allow you to describe in detail the targeted threats of information security violation of modern ICSs. Consider the threat model, constructed using EPC-diagrams as an attacker, replacing PLC control programs with the operator's workstation. In figure 2 shows the EPC-model of the information security threat of ICS violation, when an attacker penetrates the perimeter of the corporate information system segment with ICS by infecting a remote computer by malware, using identification and authentication data of a user with access to some servers of an external network segment of an industrial enterprise were compromised.

Let us analyse the attack scenario, EPC model, which is shown in figure 4.2.

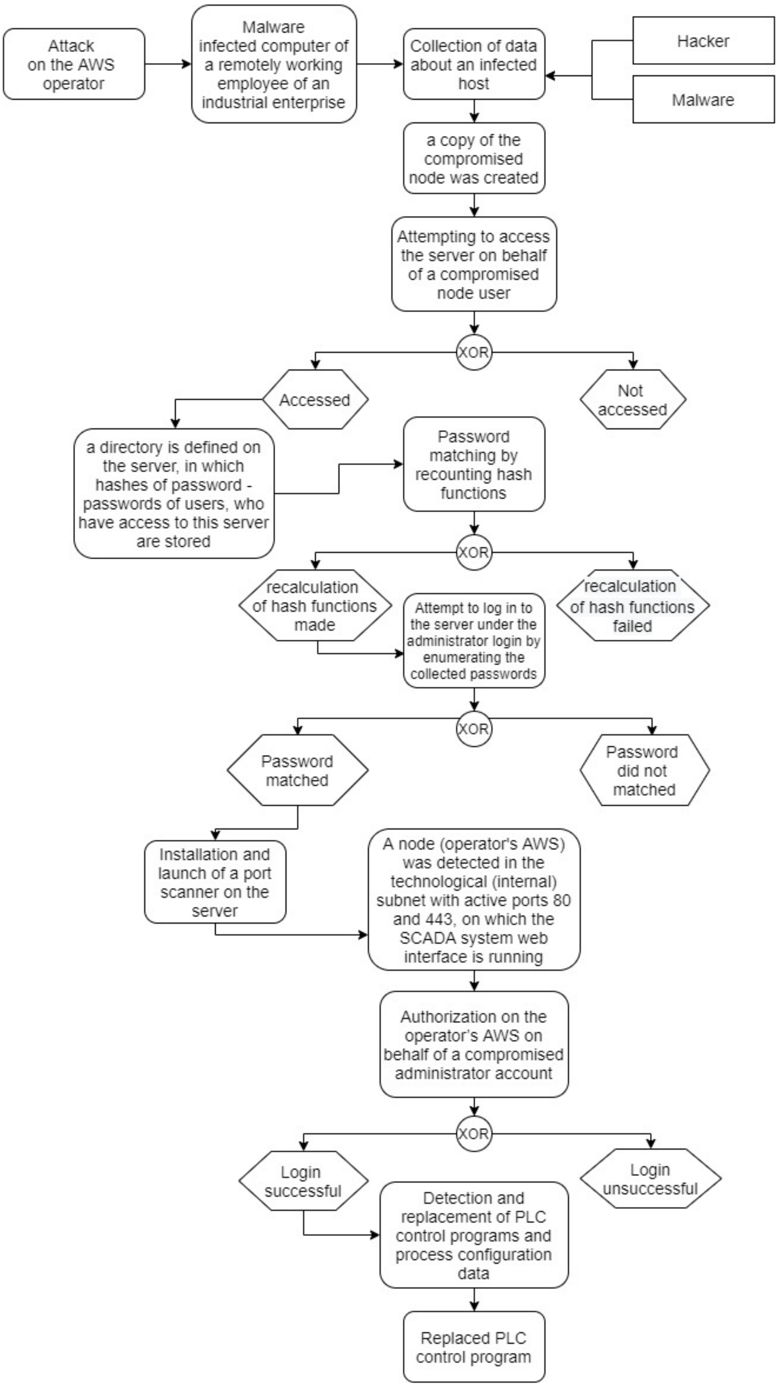

Attack on the AWS operator
Malware infected computer of a remotely working employee of an industrial enterprise
Collection of data about an infected host
Hacker
Malware
a copy of the compromised node was created
Attempting to access the server on behalf of a compromised node user
XOR
Accessed
Not accessed
a directory is defined on the server, in which hashes of password - passwords of users, who have access to this server are stored
Password matching by recounting hash functions
XOR
recalculation of hash functions made
Attempt to log in to the server under the administrator login by enumerating the collected passwords
recalculation of hash functions failed
XOR
Password matched
Password did not matched
Installation and launch of a port scanner on the server
A node (operator's AWS) was detected in the technological (internal) subnet with active ports 80 and 443, on which the SCADA system web interface is running
Authorization on the operator's AWS on behalf of a compromised administrator account
XOR
Login successful
Login unsuccessful
Detection and replacement of PLC control programs and process configuration data
Replaced PLC control program

**Figure 4.2:** EPC-model of threat of replacing the operator of PLC control programs with the operator's workstation [A.Aa]

An attacker infected a malware (Trojan) computer by an employee of an industrial enterprise working from a remote workstation. The Trojan program collected data from a compromised node (logins, passwords and data necessary for communication between the node and the industrial server on the VPN channel), then the attacker created a copy of the compromised node on his computer (using stolen data) and attempted to connect to the industrial server.

After successful authorization on the server, the attacker determines the directory, where the hash sums of the passwords of users, who have access to this server, are stored. In most cases, this is due to incorrect settings of user access rights to resources on the database servers.

The attacker selected passwords by recalculating the hash functions and tried to log in to the server using the administrator login by enumerating the collected passwords. After the attacker picked up the password for the administrator login, he uploaded the port scanner to the server and launched it. Having discovered a host (operator's workstation) in an internal (technological) subnet with an active port running Siemens SIMATIC WinCC software, an attacker tries to log in to the host on behalf of a compromised administrator account. Further, the attacker, having discovered, replaced the PLC control programs and process configuration data with the operator's workstation. The result of the attack was a situation, in which PLC control programs were replaced.

The EPC model is presented on this example, according to which it is clear that an attacker, having access to the network infrastructure of the enterprise, performs the following: scanning the local area network (LAN) for vulnerabilities (for example, open ports, through which network services of software and automation tools work) and collection of information - at the same time, account data of some employees of the enterprise may become available to him. An attacker can try to increase the privileges of a user, whose account information was intercepted and used during the attack to a level sufficient to take control not only over a particular attacked node, but also the network service of a corporate application.

By setting up remote access to the LAN node, the control of which was intercepted, an attacker can download, upload and modify some service information, for example, configuration files, control programs, telemetry data, and so on.

Such actions by cybercriminals can lead to unpredictable, sometimes even catastrophic consequences, from an accident at work, due to which the industrial enterprise will suffer material damage, to an environmental disaster with human casualties among employees and civilians, if the production was associated with dangerous ecology substances.

Consider an example in which the SCADA server became the attacked host (figure 4.3). SCADA-server is the main link in an automated process control system. Interception by an attacker of control over this node can lead to very negative consequences at the production site or where an automated process control system is used, starting from an emergency or emergency stop of the technological process and ending with a man-made disaster. It often happens that, the SCADA server and the operator's workstation are one computer. Consider an example of an attack scenario, the EPC model of which is shown in figure 4.3.

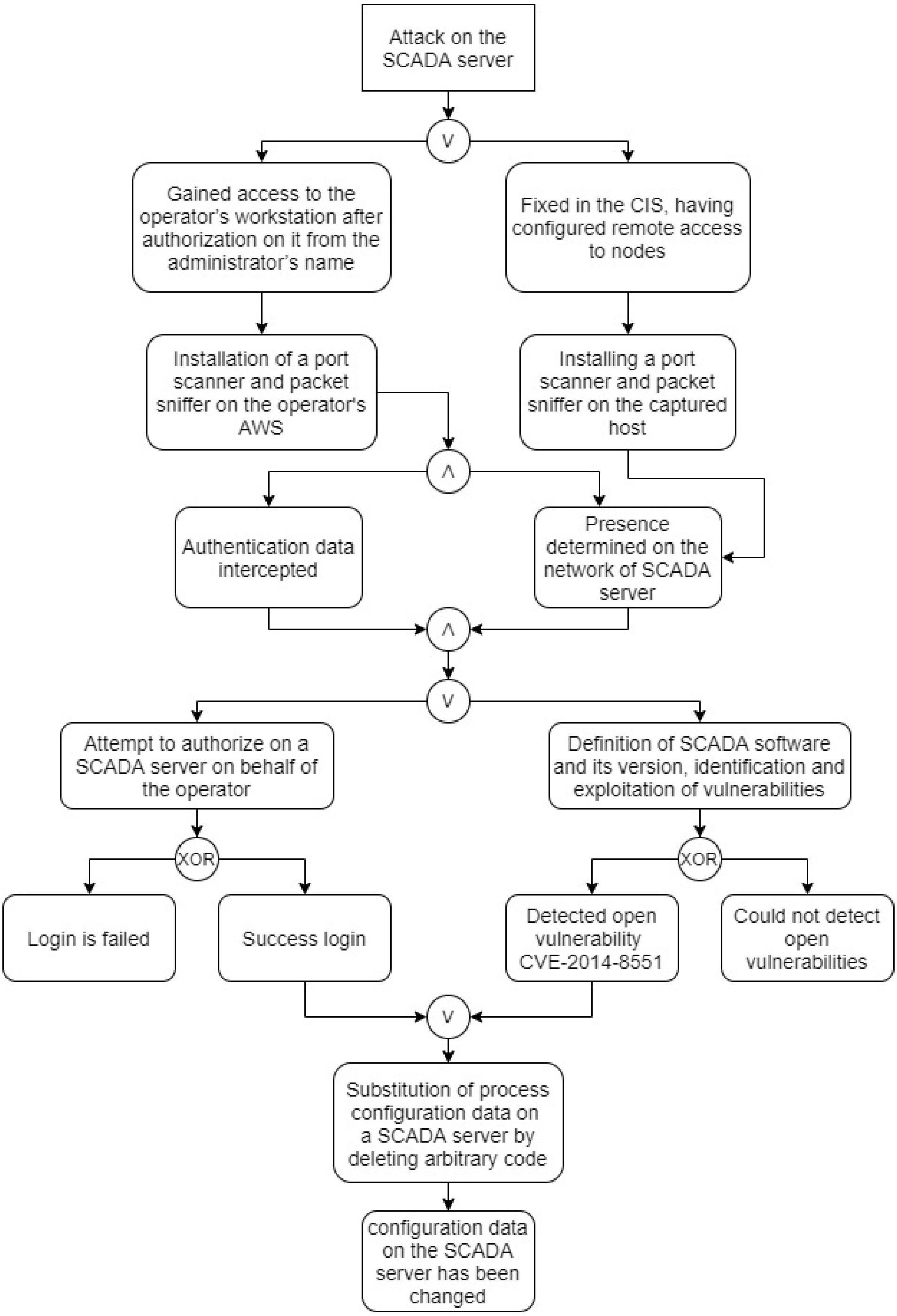

Attack on the SCADA server
V
Gained access to the operator’s workstation after authorization on it from the administrator’s name
Fixed in the CIS, having configured remote access to nodes
Installation of a port scanner and packet sniffer on the operator's AWS
Installing a port scanner and packet sniffer on the captured host
Λ
Authentication data intercepted
Presence determined on the network of SCADA server
Λ
V
Attempt to authorize on a SCADA server on behalf of the operator
Definition of SCADA software and its version, identification and exploitation of vulnerabilities
XOR
XOR
Login is failed
Success login
Detected open vulnerability CVE-2014-8551
Could not detect open vulnerabilities
V
Substitution of process configuration data on a SCADA server by deleting arbitrary code
configuration data on the SCADA server has been changed

**Figure 4.3:** EPC-model of threat of information security violation of SCADA-server [A.Aa]

An attacker installed a port scanner and packet sniffer on the operator's workstation, after which, after scanning the network, he determined the presence of the Siemens SIMATIC WinCC SCADA-system in it.

Using the vulnerability example CVE-2014-8551, an attacker launched arbitrary code without authorization on the server in order to modify the configuration of the SCADA system.

Consider the description of the vulnerability CVE-2014-8551. WinCC server allows attackers to execute arbitrary code without authorization [EN].

The introduced changes can harm the normal course of the technological process, which in the future can lead to equipment failure and even industrial accidents.

Consider an example in which an OPC server became an attacked network node (figure 4.4).

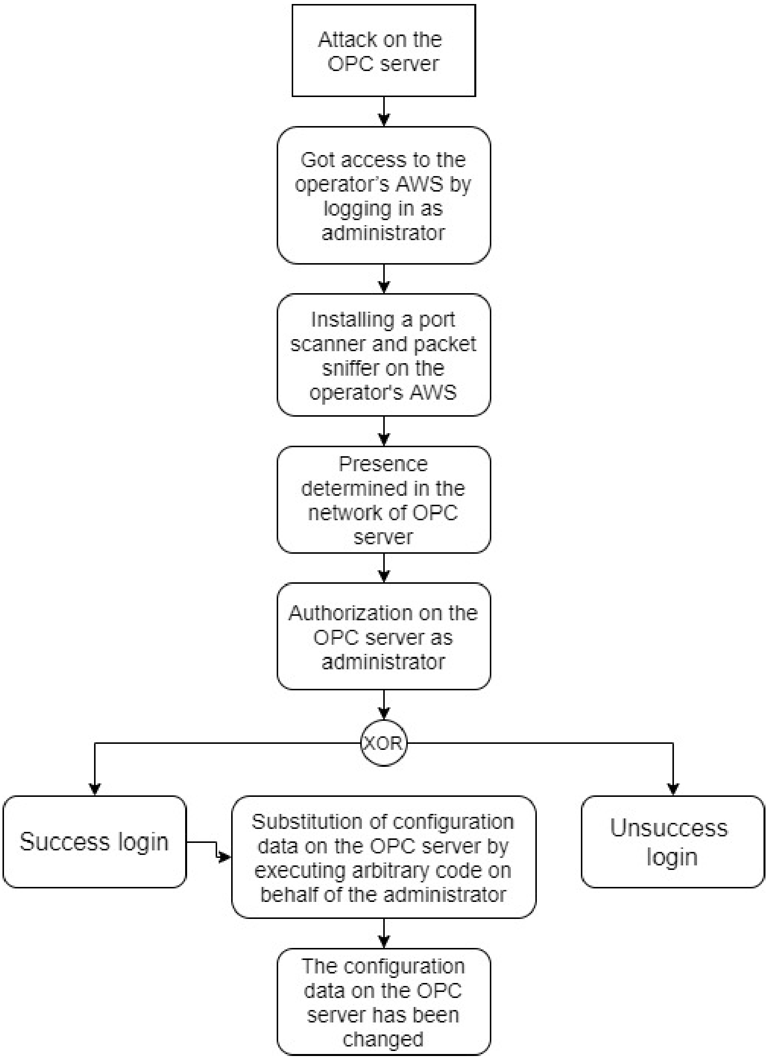

Attack on the OPC server
Got access to the operator's AWS by logging in as administrator
Installing a port scanner and packet sniffer on the operator's AWS
Presence determined in the network of OPC server
Authorization on the OPC server as administrator
XOR
Success login
Substitution of configuration data on the OPC server by executing arbitrary code on behalf of the administrator
Unsuccess login
The configuration data on the OPC server has been changed

**Figure 4.4:** PC-model of threat of violation of information security of the OPC server [A.Aa]

The purpose of OPC technology is to provide developers of industrial programs with a universal interface for exchanging data with any devices of different manufacturers using different technologies for transmitting and providing data. The functioning of the OPC is based on the client-server technology of information interaction, where the client of the OPC server is the SCADA management server. The OPC server plays an important role in the process of exchanging data between the middle and upper levels of ICSs, so its security must be implemented at the proper level.

Having made unauthorized access to the OPC server, an attacker can substitute data transmitted between the PEC and the SCADA server, and disruption of the OPC server can lead to loss of communication between the levels of the process control system.

An attacker gained access to the operator's workstation, stole data from the operator's account and committed himself to the internal subnet by setting up remote access. After scanning the network, it determined the presence of the OPC server, the attacker logged in to the OPC server on behalf of the administrator (whose login and password were stolen earlier), then, after gaining access on behalf of the administrator on the OPC server, he changed the interaction configurations of the SCADA system and PEC.

PLC is a device used for process automation. The main mode of operation of the PLC is its long-term autonomous use, sometimes in adverse environmental conditions, without maintenance and almost without human intervention.

Consider the attack scenario, the EPC model of which is shown in figure 4.5.

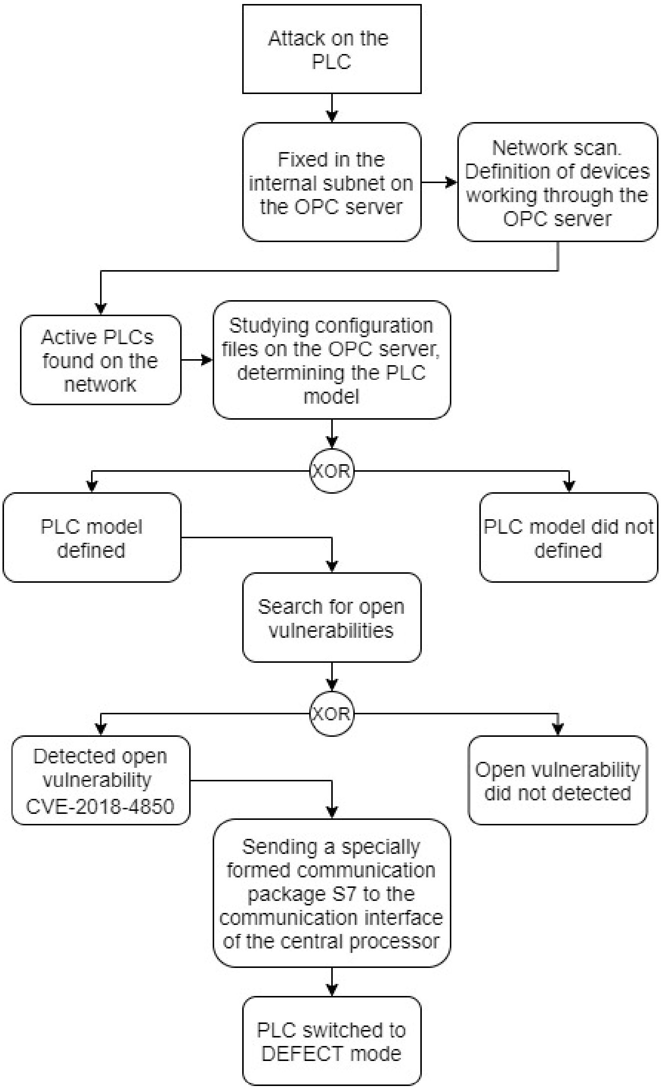

Attack on the PLC
Fixed in the internal subnet on the OPC server
Network scan. Definition of devices working through the OPC server
Active PLCs found on the network
Studying configuration files on the OPC server, determining the PLC model
XOR
PLC model defined
PLC model did not defined
Search for open vulnerabilities
XOR
Detected open vulnerability CVE-2018-4850
Open vulnerability did not detected
Sending a specially formed communication package S7 to the communication interface of the central processor
PLC switched to DEFECT mode

**Figure 4.5:** EPC model - attack on the PLC [A.Aa]

The attacker, having scanned the network, determined the presence in it of devices used in industrial automation - PLC. Having identified the PLC model, he searched for vulnerabilities on the PLC and discovered the open vulnerability CVE-2018-4850. Using it, an attacker put the PLC in DEFECT mode, after which the PLC remains in this mode until it is manually restarted.

Siemens announced the discovery of a serious vulnerability CVE-2018-4850 in a number of programmable logic controllers SIMATIC S7-400, which could lead to a denial of service [A.Ab].

SIMATIC S7-400 is a family of programmable logic controllers (PLCs) designed for process control in industry. The product is used all over the world in the areas of automotive, mechanical equipment, construction, steel production, power generation and distribution, chemical, storage, food and pharmaceutical sectors. According to Siemens representatives, these devices do not correctly check S7 packets, allowing a remote attacker to achieve denial of service by forcing the system to enter DEFECT mode and remain in it until it is manually restarted.

It follows from the Siemens message that for successful exploitation, the attacker needs to send a specially formed S7 communication package to the communication interface of the central processor. In particular, we are talking about Ethernet, PROFIBUS and Multi Point Interfaces (MPI). In particular, exploitation of the vulnerability does not require user interaction or the presence of any privileges. [A.Ab], [A.E]

There are currently no recorded cases of exploitation of this vulnerability by cybercriminals. The problem affects S7-400 processors with hardware version (HW) 4.0 and earlier, S7-400 processors with HW versions 5.0 to 5.2, and S7-400H processors with HW versions 4.5 and earlier. To fix the vulnerability, users are advised to upgrade the hardware versions to 5.0, 5.2, and 6.0, respectively [A.Ab].

Modern PLCs have a considerable number of various kinds of vulnerabilities, here is an example of the most striking of them: CVE-2014-2246, CVE-2014-2247, CVE-2014-2248, CVE-2014-2249, CVE-2014-2250, CVE-2014 -2251, CVE-2014-2252, CVE-2014-2253, CVE-2017-7899. Other currently known vulnerabilities can be viewed in the National Vulnerability Database [V.Aa].

With the development of modern technologies and their wide distribution in industrial automation control systems, more and more new vulnerabilities appear in software and hardware-software complexes of various manufacturers. Often much vulnerability is not taken into account by developers of automation systems at the production stage due to their implicit presence (for example, zero-day vulnerabilities). In most cases, they are detected at the stages of operation of these complexes directly in the systems of automated production control at industrial enterprises of customers after attacks by attackers or during an information security audit by specialists of the industrial enterprise itself. All of these vulnerabilities can be used to implement attacks in operating process control systems. As noted in [A.E], [V.Aa], threat modelling is the only way to carefully study potential destructive effects on the information environment of industrial control systems (ICSs).

## 4.2 Features of the implementation of information protection systems at ICSs

Most newly developed, designed ICSs are designed to ensure the efficiency of modern production while maintaining the reliability and safety of operation [M.Aa].

The main goal of information security in production is the safe functioning of ICSs in the normal mode within the design values. The threats and risks that may arise with the introduction of information technology without being linked to ensuring information security are indicated by the “Information Security Doctrines” in different countries. Protecting critical information infrastructure facilities is one of the three key themes of the doctrinal policy documents.

Typically, an automation object in a real sector has a developed computer network, a connection to a central object, the Internet, etc. In a typical network topology of such an enterprise, three zones are distinguished:

- Corporate - a network segment engaged in the vital processes of the enterprise itself and its officials, - ICS;
- Executive - a network segment that provides the direct implementation of technological processes (TP) of the enterprise, - ICS;
- Dispatch zone - a segment of the control system of the ICS that directly affects the progress of the TP.

Note that the information processed in the framework of these zones is different: it refers to different types of human activity, has different attributes, is regulated by a different regulatory framework and requires different approaches to conducting information security activities [G.G].

The executive zone and the dispatch zone constitute a process control system. In the executive zone there is the generation, collection, storage and processing of specialized information from a variety of industrial devices, involved in the production process. It often uses specialized software and protocols, typically, one or more systems operate in real time. In this regard, this zone has very high requirements for the reliability of the information system. Interaction with the “outside world” is not necessary for such a system.

The dispatch zone directly relates to the executive zone, since company officials (operators) from automated workstations (AWS) affect the production processes in the executive zone through interfaces removed from it. The priority task of the functioning of ICSs is to ensure the continuity of production. Until recently, it was believed that such systems, due to the uniqueness of the hardware and software configuration and their isolation and specificity, are not at all subject to unauthorized intrusions. Today it is believed that information intervention in ICSs can lead to an emergency, often with large-scale consequences. Consider the design of the information security subsystem (DISS) of the ICS segments and the key requirements for its elements and their interaction. The complex of information protection tools is a system, superimposed on existing software and hardware solutions that are used on the information resources of ICSs to be protected [G.G].

In the general case, the design of the information security subsystem of ICSs consists of the following subsystems:

- Internet working;
- Intrusion detection;
- Access control;
- Registration and accounting;
- Ensuring integrity;
- Antivirus protection;
- Security analysis;
- Information security management.

In accordance with the requirements of ensuring security and better manageability, the infrastructure of the enterprise networks is divided into several selected segments, graded according to the level of criticality and, accordingly, security. Segmentation should be carried out in such a way as to exclude the possibility of direct access from segments with a lower level of security to segments with a higher level of security. Intersegment points are protected joints according to the requirements of the guidelines. And here you need to use firewalls, certified by International organizations.

The intrusion detection subsystem identifies threats to unauthorized access during interworking. It is more convenient if these functions are built into the firewall, as well as intrusion detection mechanisms [S.Vb].

The registration and accounting subsystem captures events, related to information security. Events, occurring in the system, are recorded in the corresponding local journals, while the products used must record sufficiently detailed information in each record so that a meaningful analysis of the events can be carried out. Events occurring in the OS are also recorded by the built-in audit mechanisms and recorded in the appropriate logs. It is imperative that data from all information security event logs be timely and automatically transferred to the monitoring subsystem for further centralized processing - consolidation and analysis.

The integrity subsystem is responsible for controlling and preventing unauthorized changes in the integrity of controlled resources. Her work is based on calculating checksums and generating notifications about failures in the transmission of data packets. A mandatory element of the complex is an effective enterprise-level anti-virus protection system that detects various types of malware, is well-managed throughout the organization and supports all versions of MS Windows and Linux that are used.

The security analysis subsystem is designed to control the protection settings of operating systems on the AWS of users and servers. This subsystem should allow assessing the possibility of attackers attacking network equipment, as well as monitor the security of the software.

The information security management subsystem monitors and provides data from the point of view of work processes, maintaining their performance.

## 4.3 Methods and means of ensuring the protection of information in ICS

Most of the solutions on the market for providing information security are represented by both software and hardware tools, which require the integration into an industrial network to implement the functionality. Considering that the ICS of a gas producing enterprise is a continuous process for the extraction of natural gas, the introduction of such information security (IS) support tools in systems in which their use was not initially provided and tested can adversely affect partially or completely the entire technological process [M.Aa]. Such problems can be caused by incompatibility of hardware or software, as well as built-in blocking functionality of these tools. Based on the fact that the gas enterprise is a dangerous industrial facility, such an impact can cause equipment failure or even an accident, therefore, when choosing solutions for protecting the system, it is necessary to be guided primarily by minimal interference with production processes.

Of the classes of solutions, offered on the market that have minimal impact on the system and increase the information security of the system, the following can be distinguished [AD]:

- Firewall tools;
- One-way interworking systems;
- Intrusion detection system;
- Duplication and redirection of technological traffic;
- Correlation of incidents and monitoring of IS events;
- Vulnerability scanners;
- Threat modelling tools.

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predefined security rules. Firewalls are usually divided into network or host. Network firewalls are located on gateway computers on local area networks, wide area networks, and intranets. They represent software solutions that run on general-purpose hardware, or individual devices with an integrated OS. Host-based firewalls are located on the network node itself and control the incoming and outgoing network traffic of these devices. Each type of firewall has its own advantages and disadvantages, but in industrial networks, the network type of firewall is more often used, which is used to establish a barrier between a trusted internal network and an unreliable external network, in the case of an ICS of a producing enterprise - between an industrial network and a corporate one.

Sometimes firewall can be used inside an industrial network between the upper and middle levels to control network traffic. In this case access rules are configured in such a way that the list of open ports includes the necessary industrial protocols (for example, access is opened on the TCP port 502 (Modbus TCP).

There are also specialized industrial field firewalls (Field Firewalls, Industrial Firewalls) used at the controller level. The main vendors supplying this type of equipment are foreign companies (Siemens, Tofino-security, etc.), but domestic developments in this direction are underway.

Industrial field firewalls control industrial protocol sessions not only at the network level (which is implemented in almost every firewall), but also at the application level (a similar principle is used in some attack prevention systems, but in an extremely limited set of signatures and with a number of other restrictions), i.e. it becomes possible to assign a permissible set of function codes, for example, reading and writing to the Modbus protocol, so we get a complete inspection of industrial protocols at the application level. Modern industrial firewalls support most of the main protocols used in ICSs.

When protecting an industrial network between ICS levels, technical characteristics are also important, such as requirements for vibration loads, operating temperature, and moisture resistance. Based on certain parameters, you can determine the degree, to which the device meets the operational requirements of network equipment at a particular facility.

One-way interworking systems (also known as unidirectional gateways and data diodes) are communication devices that provide secure one-way data transfer between segmented networks. The intelligent design of such systems supports the physical and electrical separation of source and destination networks by establishing a non-routable, fully enclosed, one-way data transfer protocol between networks. Ensuring the safety of all data streams in the network using one-way gateway systems makes it impossible to transmit unsafe or hostile malware, as well as remote access to an industrial system. The technology of one-way gateways allows you to safely transmit information in only one direction, from secure areas to less secure systems, avoiding reverse access. To protect the industrial segment of the network from unauthorized access attempts by the corporate LAN segment and preserve the information interaction between the segments, data diodes are used.

An Intrusion Detection System (IDS) is a hardware or software solution that monitors a network or systems for malicious activity or security policy violations. Any malicious actions or violations are usually reported either to the administrator, or they are collected centrally using the security information and event management system (SIEM) [G.G].

The main difference between IDS and firewall is that firewall restricts access between networks to prevent intrusion and does not signal an attack within the network. Moreover, in turn IDS describes the alleged invasion after it occurred and signals a danger. Further, it also tracks attacks coming from the OS. Such capabilities are achieved by studying network interactions, identifying heuristics and signatures of common computer attacks and taking measures to prevent operators.

Types of IDS vary from individual computers to large networks. The most common classifications are Network Intrusion Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS). A system that keeps track of important operating system files is an example of HIDS and a system that analyses incoming network traffic is an example of NIDS. It is also possible to classify IDSs using the detection approach: the most well-known options are signature detection (recognition of dangerous signatures, such as malware or attacks); and detection based on anomalies (detection of deviations from the model of "good" traffic, which is often used for machine learning). Some IDS products are capable of responding to detected intrusions, such systems are called Intrusion Prevention System (IPS). The use of IPS in industrial networks is fraught with a potential blocking of the technological process in case of abnormal activity, which can significantly affect the entire industrial network as a whole, so the use of IDS with the inability to respond to detected intrusions is a more acceptable option. Thus, the formation of a demilitarized zone at the level of the network perimeter with the use of IDS can significantly increase the level of network security without affecting the process itself.

Duplication and redirection of network packets is called mirroring. Typically, port mirroring is used on a network switch to send copies of all or a single VLAN of incoming and/or outgoing network packets, received on one or more ports to a separate interface for monitoring network traffic. From the point of view of safety, this method can most effectively be used in conjunction with the previous means of protection IDS. The method is most acceptable when used in industrial IDS networks, as this ensures that when analysing traffic, there are no threats to the operation of the industrial network.

Another useful application of port mirroring is to analyse and debug received information or diagnose network errors. This helps administrators closely monitor network performance and alert them when problems occur.

In the field of computer security, security information and event management (SIEM) software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts, generated by applications and network equipment.

SIEM can represent a software or hardware solution, as well as a provided service [S.Vb]. This class of solutions can perform the following functions and components:

- Data aggregation - collection and processing of data from several sources, including network devices, servers, databases, applications, security logs, providing the ability to consolidate monitored data so, that important events do not go unnoticed;
- Correlation - the search for common attributes and combining events into meaningful connectives, which provides the ability to perform various methods of searching for the relationship when integrating various sources, so that information about events is the most complete and does not contain repetitions;
- Alert - an automated analysis of processed events with a custom notification of incidents;
- Toolbars - real-time monitoring tools that can collect data about events and turn them into information diagrams to visualize the ability to track patterns or identify actions, that are abnormal;

- Compliance check - the system can be used to automate the verification of collected data for compliance with security requirements, to prepare reports that are adapted to existing processes or security audits;
- Storage - the use of long-term storage of irrelevant data to more accurately correlate data over time, as well as to investigate potential incidents;
- Forensic analysis - the ability to search through the event logs of available network nodes at various time intervals, based on certain criteria.

The focus is on monitoring and managing user and service rights, directory services and other system configuration changes and incident response.

The SIEM system combines output from several sources and uses alarm filtering methods to distinguish malicious activity from false alarms, which eliminates the need to monitor various security consoles and manually analyse the events, received from them, automating and simplifying this process as much as possible. Vulnerability scanner is a computer program, designed to evaluate computers, network infrastructure or applications for known vulnerabilities. They are used to identify and detect vulnerabilities, arising from incorrect configuration or errors in the program code of network devices and programs, such as firewalls, routers, web servers, application servers and so on. Modern vulnerability scanners allow scanning both with and without authentication. Most vulnerability scanners have the ability to generate vulnerability reports, as well as installed software, open ports, certificates, and other device information that can be requested during the scan.

Authentication scanning allows the scanner to directly access network resources using remote administration protocols, such as SSH or UDP and authenticate using the provided system credentials. This allows the vulnerability scanner to access low-level data, such as specific services and device OS configuration information. After scanning, detailed and accurate information about the OS and installed software is provided, including configuration flaws and missing security fixes.

Scanning without authentication is a method that can lead to a large number of false positives and does not allow providing detailed information about certain services and OS configuration, as well as installed software. This method is commonly used by threat actors or security analysts trying to determine the security status of external available assets.

Threat modelling is the process, by which potential threats, such as structural vulnerabilities, can be identified, listed and prioritized at the earliest stage of design - from the point of view of a hypothetical attacker. The goal of threat modelling is to provide information security professionals with a systematic analysis of the profile of a likely attacker, the most likely attack vectors and assets prone to a more likely attack. Unlike vulnerability scanners, threat modelling tools do not need to interact with devices to analyse current vulnerabilities.

Typically, IT-related threat modelling processes begin by creating a visual representation of the analysed application or network infrastructure. An application or infrastructure is divided into separate elements in order to analyse the most detailed analysis of the entire system as a whole. After the analysis is complete, a visual representation is used to list potential threats. Further analysis of the model in relation to risks associated with identified threats, prioritization of threats and listing of appropriate mitigating management measures depends on the methodological basis of the used threat model process [M.Ac].

Threat modelling should preferably be performed in the early stages of the design cycle, when potential problems can be identified in the early stages and eliminated, which will avoid a more costly solution to the problem in the future. Using threat modelling to analyse security requirements can lead to proactive architectural solutions that can help reduce threats from the start of system operation.

**Comparison of the considered classes of solutions**

To select the safest solution for providing IS ICS, it is necessary to create a list of criteria for comparing the classes considered. Thus, the following characteristics will be used as criteria:

- Impact on industrial traffic;
- Work at all levels of ICS;
- Change the settings of the equipment used;
- Use of this class of solutions in the designed process control system.

Based on the listed criteria, a comparison was made of the considered Classes of solutions in table 4.1.

| | **Impact on Industrial Traffic** | **Work at all levels of ICS** | **Changing the settings of the equipment used** | **Use in the designed ICS** |
|---|---|---|---|---|
| **Firewall funds** | Yes | Yes | No | No |
| **Data diode** | Yes | Yes | No | No |
| **IDS** | Yes | Yes | Yes | No |
| **Traffic mirroring** | No | Yes | Yes | No |
| **SIEM system** | Yes | No | Yes | No |
| **Vulnerability Scanners** | Yes | No | Yes | No |
| **Threat Modelling Tools** | No | Yes | No | Yes |

**Table 4.1:** Comparison of the current classes of solutions for providing information security of ICS [M.Ac]

The installation and configuration of information protection tools is carried out in cases where such tools are necessary to neutralize information security threats that cannot be ruled out by setting up an ICS. Thus, if we take into account the results of comparing the classes of solutions (Table 4.1), where only threat modelling tools, do not require any manipulations with the working system (such as setting up network equipment and introducing additional software or hardware and software solutions into an industrial network). Then first of all, it is necessary to use the built-in functionality of an automated system to increase security, including the elimination of vulnerabilities in the current infrastructure. Threat modelling tools are the safest tool that can increase the IS level of a production system. It should also be noted that such tools make it possible to efficiently design an industrial network that does not yet exist, eliminating potential threats in the early stages.

# Chapter 5
# INTRODUCTION OF AN INTEGRATED INFORMATION SECURITY SYSTEM

## 5.1 Analysis and selection of software information protection

The most effective approach to protecting against information leakage from computers begins with the use, first of all, of contextual control mechanisms - prohibition or permission to transfer data for specific users depending on data formats, types of interfaces and devices, network protocols, transmission direction, day of the week and time days, etc. [AD].

However, in many cases, a deeper level of control is required - for example, checking the contents of the transmitted data for personal or confidential information in conditions where the income/outcome (I/O) ports should not be blocked so as not to disrupt production processes, but individual users are included in the "risk group", because they are suspected of involvement in violations of the corporate information security policy. In such situations, in addition to contextual monitoring, it is necessary to use technologies of content analysis and filtering to identify and prevent the transfer of unauthorized data, without interfering with the information exchange within the framework of official duties of employees [A.Va].

In order for the data loss prevention (DLP) system to be able to distinguish between different categories of information, it is necessary to establish and transfer these rules to the system. Modern leakage protection systems have a generated data dictionary and a set of rules for detecting data of various types and a list of actions for such detection. However, this does not eliminate the need for fine-tuning the system, taking into account the characteristics of the data processed in a particular company.

Currently, a large number of DLP systems are on the market. Let us consider for comparison some of them, namely:

- Zecurion DLP;
- Watch Jet 4.0.24;
- Symantec Data Loss Prevention;
- Garda Enterprise.

You can compare products by several criteria:

- market positioning of the system;
- system requirements;
- used detection technologies;
- controlled data transmission channels;
- the ability to control connected external devices;
- system management and incident handling;
- reporting.

In order to choose a DLP system for implementation, we will use the hierarchy analysis method [AD]. This method is a mathematical tool that allows you to apply a systematic approach to multi-criteria decision-making problems. This method allows you to interactively determine which solution to the problem is most consistent with the requirements that are defined for its solution.

This method is applied in the following order:

1. First, the goal and options for achieving it are determined;

2. A problem model is constructed in the form of a hierarchy with the definition of criteria for identifying the quality of alternatives;

3. The priority of each criterion and each element of the hierarchy is determined by the method of pairwise comparison;

4. Identification of global priorities of options by comparing priority criteria;

5. Determining the correctness of the conclusions made;

6. Determination of the preferred option based on the study.

The purpose of the comparison in this case is to select the most appropriate DLP system to prevent leaks in the company's information system. To do this, we compare three of the four previously considered information leakage protection systems, namely Zecurion DLP, Symantec DLP, and Garda Enterprise with ten independent characteristics (three leakage channels, six methods of preventing information leakage, and certification). The data that an expert need to determine the functionality of each of the systems for this comparison is obtained from the manufacturers websites, from the documentation and from testing the evaluation versions of the programs.

Matrices of pairwise comparisons are compiled to determine priorities (table 5.1). Expert data is formulated on the basis of the above information (characteristics of the compared DLP systems and ideas about the protected object). Comparisons were carried out on a scale of significance from 1 to 9 (1 - equal importance, 3 - slight superiority, etc., inverse values - if the compared object is inferior in this characteristic).

| | **Channel 1** | **Channel 2** | **Channel 3** | **Method 1** | **Method 2** | **Method 3** | **Method 4** | **Method 5** | **Method 6** | **Certification** |
|---|---|---|---|---|---|---|---|---|---|---|
| **Channel 1** | 1 | 1/3 | 1/5 | 1 | 1 | 1 | 1 | 1 | 1 | 1/3 |
| **Channel 2** | 3 | 1 | 1/3 | 1 | 1 | 1 | 1 | 1 | 1 | 1/3 |
| **Channel 3** | 5 | 3 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1/3 |
| **Method 1** | 1 | 1 | 1 | 1 | 1/9 | 1/7 | 1/7 | 1/7 | 1/7 | 1/3 |
| **Method 2** | 1 | 1 | 1 | 9 | 1 | 5 | 3 | 1 | 3 | 1/3 |
| **Method 3** | 1 | 1 | 1 | 7 | 1/5 | 1 | 1 | 1/5 | 1/7 | 1/3 |
| **Method 4** | 1 | 1 | 1 | 7 | 1/3 | 1 | 1 | 1/5 | 1/7 | 1/3 |
| **Method 5** | 1 | 1 | 1 | 7 | 1 | 5 | 5 | 1 | 1/3 | 1/3 |
| **Method 6** | 1 | 1 | 1 | 7 | 1/3 | 7 | 7 | 3 | 1 | 1/3 |
| **Certification** | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 1 |

**Table 5.1:** Matrix of pairwise comparisons [AD]

**Hardware and software complex "Garda Enterprise".** This solution is a DLP system, designed to control confidential information leaks, investigate related incidents and solve other problems. The product in question is universal. This means that it is both a gateway and a host. This allows you to control with its help both local and network channels of leakage of confidential information. To date, the solution in question can control all the main channels of corporate communications - email, IM-systems, IP-telephony, Internet services (social networks, forums, blogs, chats, etc.), file transfer services (FTP, P2P, etc.), removable drives that run programs and applications at the workplace, as well as external devices, in particular, local and network printers and faxes [MV].

An important feature of the product in question is its specialization. Today, the Garda Enterprise DLP system remains one of the most powerful solutions, as it is specially designed for use in large and medium-sized institutions. The solution provides very high performance, up to 10 Gb/s and higher. The developer of the hardware and software complex "Garda Enterprise", "MFI Soft", is a well-known manufacturer on the market of carrier-level systems, including SORM systems and solutions for protection against DDoS attacks. And who, if not the specialists of this company, should have extensive experience in the field of high-performance network applications [FST].

The solution in question works with mirrored traffic. That is, its installation "in the gap" and work in filtering mode is not considered. On the one hand, this reduces the functionality of the system. However, it should be borne in mind that in practice in medium and large companies filtering is extremely rarely used. In the vast majority of cases, DLP systems in them are used to "listen" to traffic, that is, to monitor leaks, investigate incidents, identify disloyal employees and solve other common problems. Therefore, the absence of a filtration mode in the solution, strictly speaking, cannot be considered a serious drawback [NJ].

The hardware and software complex "Garda Enterprise" are delivered in the form of a ready-made hardware-software complex, which includes a server and software installed on it. Such a solution is convenient in that the consumer receives a ready-to-launch solution that fully meets the needs of the customer and allows for its implementation in the shortest possible time. However, if a potential customer already has a hardware platform, the product can also be sold as software.

The composition of the hardware and software complex "Garda Enterprise" includes the following modules (figure 5.1):

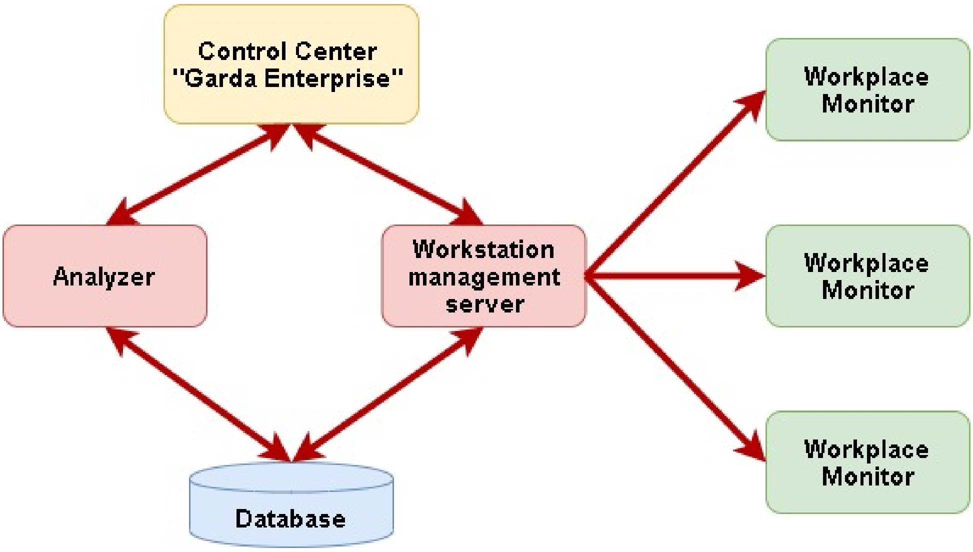


**Figure 5.1:** The composition of the hardware and software complex "Garda Enterprise" [NJ]

- Analyzer - a hardware-software complex, designed to intercept and analyze traffic;
- Database - Data Base Management System (DBMS) with a database in which all system information is stored;
- Workstation management server - a hardware-software complex for managing agents at workstations;
- Workplace Monitor - an agent program, installed on workstations;
- Control Center "Garda Enterprise" - software for the system administrator and security administrators.

The system can run several analyzers that will collect information in a single database. This allows you to build a high-performance and distributed system of protection against leakage of confidential information.

The hardware-software complex "Garda Enterprise" is supplied as a ready-made hardware-software complex, the configuration of which is calculated based on the needs of a particular client. Therefore, it makes no sense to cite any system requirements for the server components of the system.

I would like to point out that I have provided detailed information on one of the DLP systems in order to show how this system works and can serve the purpose of this general work perfectly. Any of the DLP systems can be used as a means of protecting against data loss. DLP systems solutions are a future that needs to be addressed today.

## 5.2 Analysis and selection of cryptographic information security tools

To increase the level of information security, it is necessary to apply ViPNet technology. ViPNet technology performs the functions of a firewall both for open connections and for secure ones, an intrusion detection system (IDS), an IM client, an email service (protected from spam and unauthorized access) and assignment of virtual visibility addresses [LF].

The fundamental difference between ViPNet technology and most modern virtual private network (VPN) systems, which are mainly designed for secure connection of local networks and remote access to their resources, is the existence of special protocols for dynamic routing of VPN traffic. These protocols make it possible to ensure automatically the secure exchange of information not only with a VPN gateway, installed on the local network boundary, but also directly between end-users of information [A.Ab].

An important feature of ViPNet technology is the use of a symmetric key structure for VPN, which allows you to get rid of periodic authentication sessions of network nodes and key generation procedures. These operations are necessary in systems with an open key distribution; however, they complicate the use of VPNs in local networks and reduce the noise immunity of a communication session due to the possibility of its violation at the synchronization stage [A.E]. ViPNet networks do not need to deploy the sophisticated public key infrastructure (PKI) necessary to safely use an asymmetric key structure. The difference between ViPNet solutions and most modern VPN systems, which can also work with symmetric keys, is the presence of an automated system for managing symmetric key information [RB].

To implement ViPNet networks, it will be enough to install the appropriate ViPNet software on the workstations. Also, it will not be necessary to change the topology of the already created network or buy additional equipment. When organizing a secure connection, ViPNet technology uses a scheme with automatically distributed symmetric encryption keys and automatically updates them at the stages of software installation. Any packet that is sent to the network, is encrypted using a unique key without any connection establishment procedures. This helps to successfully organize the transmission of information through unprotected channels, as well as through channels that are characterized by large traffic losses (satellite, modem), and also allows for continuous LAN operation, for which delays in establishing a connection are unacceptable [ASa].

The cryptographic provider **ViPNet CSP** is a cryptographic data protection tool, designed to implement cryptographic operations that can be accessed by embedding the cryptographic provider in the application itself through a specialized interface. ViPNet CSP supports cryptographic algorithms that fully comply with standards [J.S].

**ViPNet SafeDisk** is used to implement the technology of safe storage of classified information and convenient work with it on a regular PC. Version 4 maintains a high level of security of any data and can be successfully used in government agencies and companies as a cryptographic information protection measure and a security tool against unauthorized access to data [V.Ab].

**ViPNet OFFICE** is a comprehensive software for deploying virtual private secure networks (VPN) of standard models - ViPNet secure networks. In turn, ViPNet OFFICE is also used in small local and distributed IP networks and allows secure operation of remote users with different types of Internet connections.

**ViPNet Office Firewall** is a software firewall that is used in small and medium-sized organizations and is a means of protection from illegal actions with confidential data [SVa]. ViPNet Office Firewall gives you the opportunity to implement LAN protection from any attacks from the Internet, and also has mechanisms for flexible access control to Internet resources and support for virtual local networks.

**ViPNet Personal Firewall** is a reliable means of protecting the workstation and personal data from network attacks and identity theft when connected to the Internet or LAN [Sta]. ViPNet Personal Firewall is a means of protecting data from unauthorized access and can be used by government agencies and enterprises.

The following software is required for each workstation:

- ViPNet SafeDisk (certified);
- ViPNet OFFICE;
- ViPNet Personal Firewall (certified).

You also need to purchase a server to install the following software:

- ViPNet CSP;

- ViPNet Office Firewall (certified).

The ViPNet CUSTOM software package allows you to create an environment for the safe exchange of information through publicly available communication channels of various types [P.A].

A typical ViPNet network diagram is shown in figure 5.2.

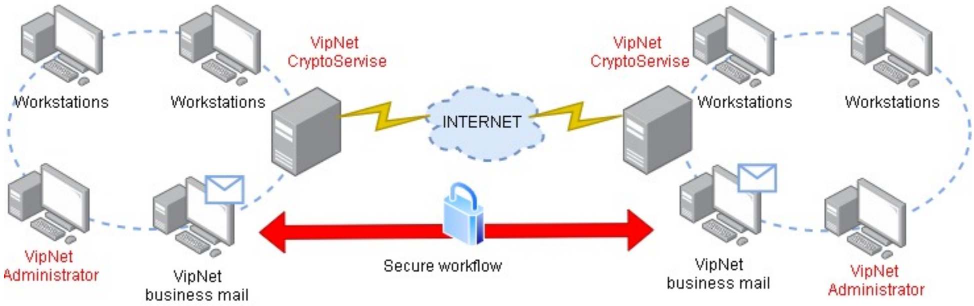


**Figure 5.2:** Typical ViPNet Network Diagram [A.O]

The second type of ViPNet network loop is modified from the first by adding the necessary licenses and installing the necessary software. This type of circuit allows the use of private virtual networks of various configurations that support the visual interaction of a PC in the ViPNet network, regardless of the location, method and type of IP address, when connecting to the network. Moreover, all traffic, transmitted along the virtual circuit of this network, is encrypted using cryptographic methods [Lawa].

To maintain the full security of the corporate LAN, you need to install ViPNet software, which helps to save not only messages, transmitted over the network, but also all network traffic, as well as data stored locally on the PC. Moreover, access to such a PC from unsafe or other secure computers is otherwise restricted and controlled [Lawb].

The organization of such protection requires the following basic network elements: [P.A]

- The workplace of the administrator of the ViPNet network with the installed software;

- ViPNet Administrator, which consists of two components;
- ViPNet Network Management Center (NMC);
- ViPNet Certification and Key Center (CKC);
- ViPNet Client or ViPNet CryptoService for organizing the exchange of service information with other nodes of the ViPNet network;
- Server(s) with ViPNet Coordinator installed, located at the network boundary or at the boundaries of network sections. Depending on its role in the network, the coordinator can perform various functions [MH];
- Computers of users with installed client software ViPNet Client or ViPNet CryptoService.

In addition to the listed basic elements, other functional components can be present on the ViPNet network that solve backup, monitoring, certificate sharing and others. Types of ViPNet software, depending on the purpose and role in the network, are presented in figure 5.3.

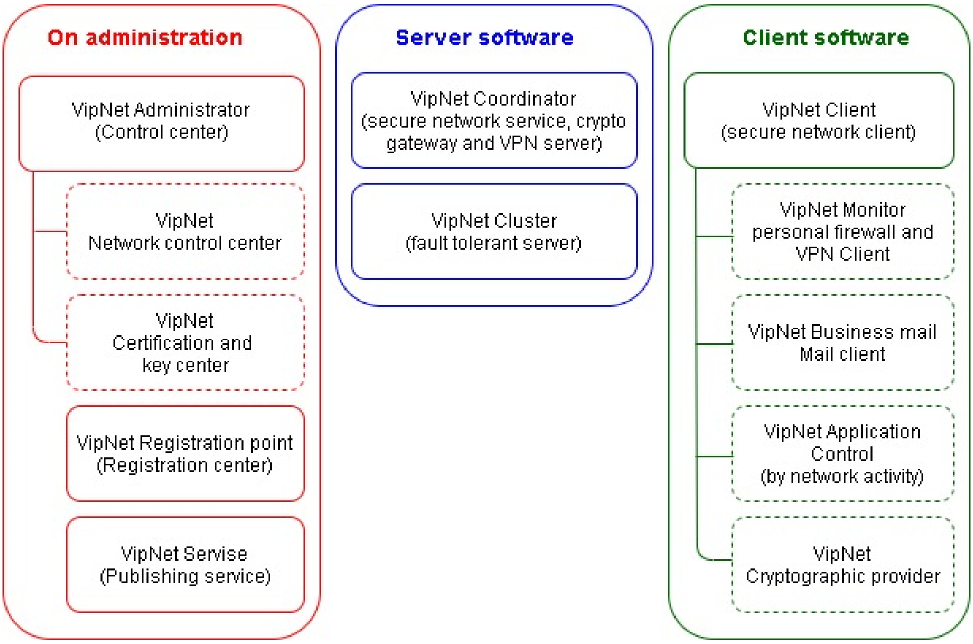

On administration
VipNet Administrator (Control center)
VipNet Network control center
VipNet Certification and key center
VipNet Registration point (Registration center)
VipNet Servise (Publishing service)
Server software
VipNet Coordinator (secure network service, crypto gateway and VPN server)
VipNet Cluster (fault tolerant server)
Client software
VipNet Client (secure network client)
VipNet Monitor personal firewall and VPN Client
VipNet Business mail Mail client
VipNet Application Control (by network activity)
VipNet Cryptographic provider

**Figure 5.3:** Types of ViPNet software [A.O]

The network includes the following components [A.O]:

**ViPNet Network Management Center (NMC)**

The main component of the ViPNet network must perform the following functions:

- Development and modification of the topology of the ViPNet network;
- Differentiation of access and user rights within the network;
- Transfer of keys, received from the certification and key center (CKC), updates and information about the network topology to network nodes;
- Implementation of applied tasks: “network control center”, “traffic protection”.

**ViPNet Certification and Key Center (CKC)**

ViPNet: CKC - is a required component of the ViPNet network and performs the following functions:

- Creating custom keys to protect data [V.F];
- Implement and manage user certificates.

The CKC itself in the ViPNet network only interacts with the NMC - it receives data from it about nodes and users in the network, sends key data to protect information. For security reasons, you should not connect a PC with a CKC to the ViPNet shared network, but only implement its connection with the central control center computer.

Applied tasks: “Identity and key center”, “Traffic protection” [A.E].

**ViPNet Coordinator**

ViPNet Coordinator is a required component of the ViPNet network. The node with ViPNet Coordinator software in accordance with the tasks can implement the following functions:

- Implementing a secure connection between secure networks through a public network (proxying);
- Installing a firewall to filter open and tunneled traffic;

- Notification of nodes about mutual parameters of each other (IP address server);
- Implementation of secure interaction between open resources in the LAN;
- Performing the function of mail servers for the Business Mail software and coordination from the central control center;
- Implementation of a secure Internet connection in full accordance in the field of international information exchange".

The set of applied tasks, that are assigned to the coordinator, may be different, depending on its role and the functions, implemented in the network.

**ViPNet Client**

The node with ViPNet Client software allows you to perform the following functions:

- Filtering open traffic, using a personal firewall;
- Encryption of PC network traffic;
- Providing additional service functions for quick encryption of sent messages, conferences, file sharing, etc.;
- Providing statistics and monitoring tools;
- Implementation of secure transfer of electronic documents;
- Implementation of protection against unauthorized activity of software, installed on the computer.

The technical support scheme taking into account the elements of the designed information security system between the main office and branches is shown in figure 5.4.

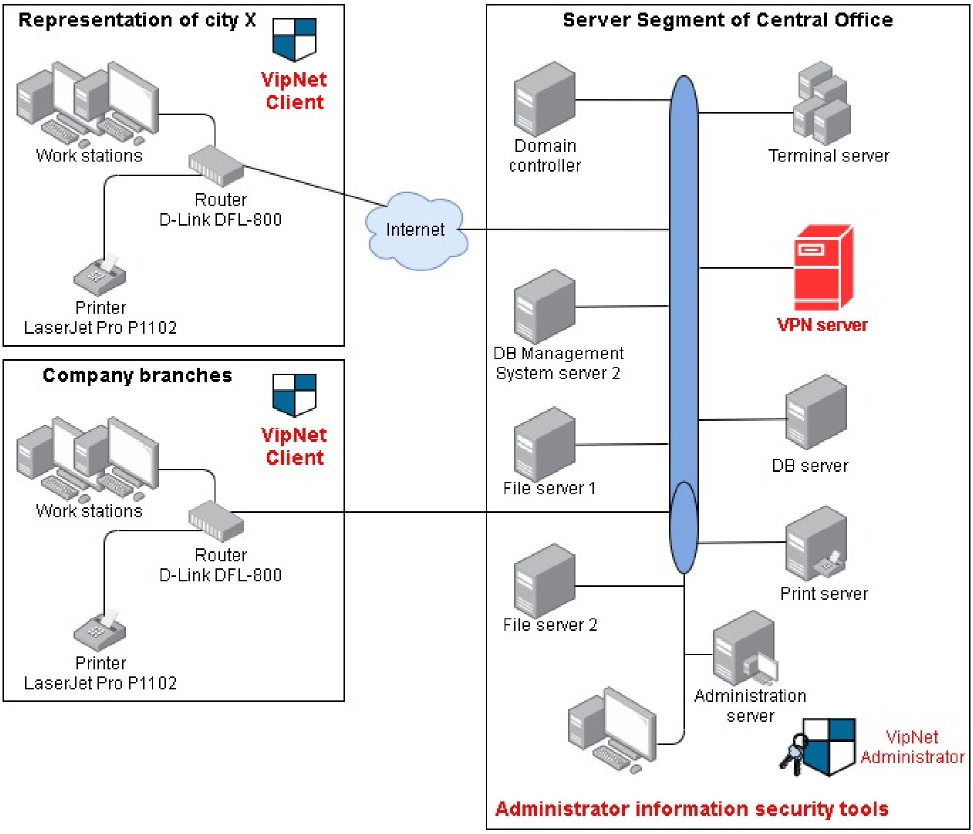


**Figure 5.4:** Software block diagram for VPN system elements [V.F]

# Chapter 6 PRACTICAL PART

## 6.1 Vulnerable Internet devices

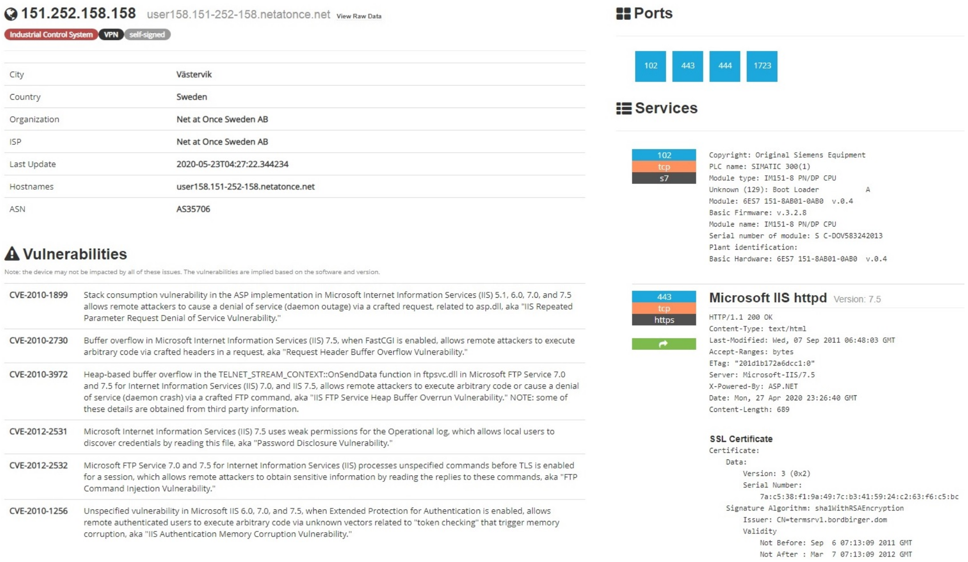
In the CHAPER 4, we talked about potential threats to industrial control systems (ICSs), explored possible scenarios for how a hacker could hack ICS systems, identified the biggest problems and errors that still occur in configuring various Internet devices and the lack of proper protection. We also provide the names of the most vulnerable devices, their models, software and hardware versions and which hardware are more vulnerable. All that remains is to practically check and make sure that ICSs are still at risk today?!

I chose the search system - SHODAN - to check the vulnerability of the ICS. Shodan is a computer search engine that lets the user find IT systems such as servers, routers, network switches, desktops, printers, webcams and etc., connected to the internet [Wil]. The web site: https://www.shodan.io. I used Shodan and article Shodan Eye. Shodan Eye is a public tool to use by Linux terminal. I made search by countries and got info, which is published in table 5.1. A study has shown that many vulnerable systems still exist on the Internet today (Figure 5.1). Starting the research, I did a PLC (Programmable Logic Controller) search on the internet. The results obtained are shown in table 6.1.

| Country | Found PLCs |
|---|---|
| China | 1308 |
| Germany | 1020 |
| Italy | 865 |
| USA | 658 |
| Sri Lanka | 656 |
| ... | ... |
| Norway | 57 |
| Sweden | 36 |
| Denmark | 26 |
| Finland | 4 |
| **All:** | **7083** |

**Table 6.1:** PLC in Internet with opened ports [SHO]

As we can see from the data, presented in table 6.1, a total of 7083 PLCs with open ports were detected. Of them - 1942, which use Siemens S7 hardware (we have already talked about the vulnerability of this equipment in the previous section). The largest number of PLCs with open ports is in China - 1308. In Norway - 57.



151.252.158.158 user158.151-252-158.netatonce.net

| | |
|---|---|
| City | Västervik |
| Country | Sweden |
| Organization | Net at Once Sweden AB |
| ISP | Net at Once Sweden AB |
| Last Update | 2020-05-23T04:27:22.344234 |
| Hostnames | user158.151-252-158.netatonce.net |
| ASN | AS35706 |

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

| | |
|---|---|
| CVE-2010-1899 | Stack consumption vulnerability in the ASP implementation in Microsoft Internet Information Services (IIS) 5.1, 6.0, 7.0, and 7.5 allows remote attackers to cause a denial of service (daemon outage) via a crafted request, related to asp.dll, aka "IIS Repeated Parameter Request Denial of Service Vulnerability." |
| CVE-2010-2730 | Buffer overflow in Microsoft Internet Information Services (IIS) 7.5, when FastCGI is enabled, allows remote attackers to execute arbitrary code via crafted headers in a request, aka "Request Header Buffer Overflow Vulnerability." |
| CVE-2010-3972 | Heap-based buffer overflow in the TELNET_STREAM_CONTEXT::OnSendData function in ftpsvc.dll in Microsoft FTP Service 7.0 and 7.5 for Internet Information Services (IIS) 7.0, and IIS 7.5, allows remote attackers to execute arbitrary code or cause a denial of service (daemon crash) via a crafted FTP command, aka "IIS FTP Service Heap Buffer Overrun Vulnerability." NOTE: some of these details are obtained from third party information. |
| CVE-2012-2531 | Microsoft Internet Information Services (IIS) 7.5 uses weak permissions for the Operational log, which allows local users to discover credentials by reading this file, aka "Password Disclosure Vulnerability." |
| CVE-2012-2532 | Microsoft FTP Service 7.0 and 7.5 for Internet Information Services (IIS) processes unspecified commands before TLS is enabled for a session, which allows remote attackers to obtain sensitive information by reading the replies to these commands, aka "FTP Command Injection Vulnerability." |
| CVE-2010-1256 | Unspecified vulnerability in Microsoft IIS 6.0, 7.0, and 7.5, when Extended Protection for Authentication is enabled, allows remote authenticated users to execute arbitrary code via unknown vectors related to "token checking" that trigger memory corruption, aka "IIS Authentication Memory Corruption Vulnerability." |

```
Copyright: Original Siemens Equipment
PLC name: SIMATIC 300(1)
Module type: IM151-8 PN/DP CPU
Unknown (129): Boot Loader          A
Module: 6ES7 151-8AB01-0AB0  v.0.4
Basic Firmware: v.3.2.8
Module name: IM151-8 PN/DP CPU
Serial number of module: S C-DOV583242013
Plant identification:
Basic Hardware: 6ES7 151-8AB01-0AB0  v.0.4
```

Microsoft IIS httpd Version: 7.5

```
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 07 Sep 2011 06:48:03 GMT
Accept-Ranges: bytes
ETag: "201d1b172a6dcc1:0"
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Mon, 27 Apr 2020 23:26:40 GMT
Content-Length: 689
```

SSL Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            7a:c5:38:f1:9a:49:7c:b3:41:59:24:c2:63:f6:c5:bc
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=termsrv1.bordbirger.dom
        Validity
            Not Before: Sep  6 07:13:09 2011 GMT
            Not After : Mar  7 07:13:09 2012 GMT
```

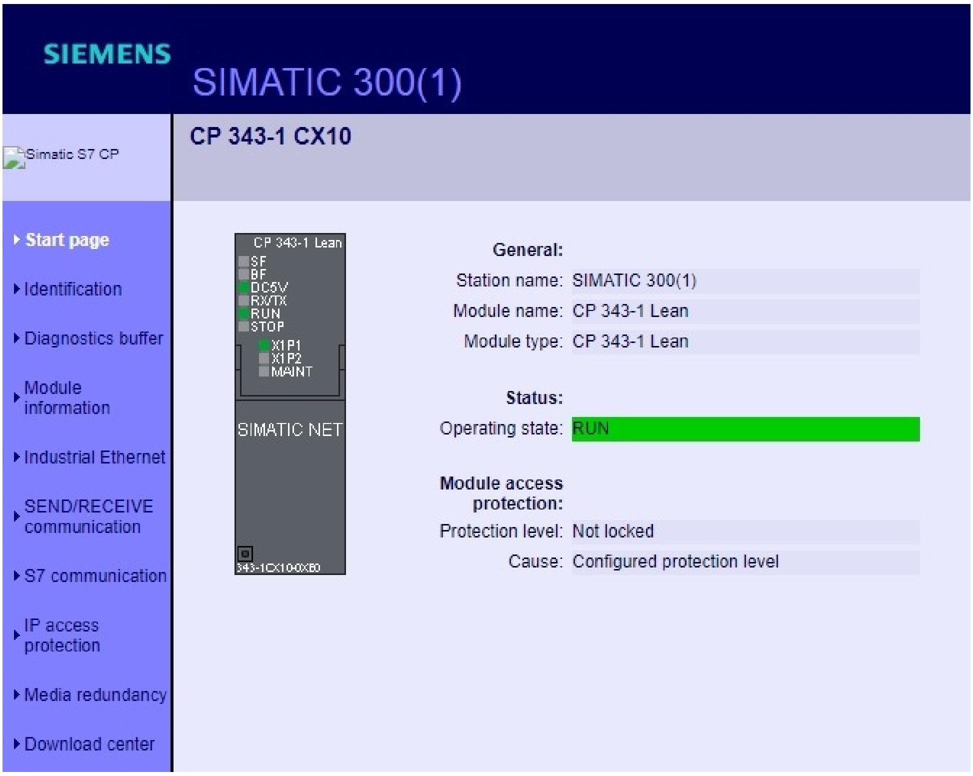
**Figure 6.1:** Vulnerabilities of ICS [SHO]

The next step of this investigation was to check their security and try to find a loophole in the configuration. Unfortunately, vulnerabilities have been found here as well. In addition to the identification system, we connected to the Siemens S7 SIMATIC 300 system (figure 6.2) and the turbine control system (figure 6.3).

In figure 6.2 available to go through menu and get much info about device: module, hardware, version, other IP addresses and ports related to this device. This info is beginning of research for hacker. In particular, this information should not be available to every user. The port should not be open. And an identification system should be applied here. At the very least, in order to log in to the system and see the information, the user would have to log in with a certain username and password. And the administrator should determine the user's responsibilities, rules for working with the information. This would be a minimum requirement to protect this system and information from public access.

In figure 6.3 have to be available to change settings in settings menu, but I did not try as it is illegal, just walked though menu. It should be noted that no identification is required to connect to these systems. This can be considered a very group violation in the protection of ICS systems. Obviously, the information available is not for the average user. Changing the parameters in the menu settings is likely to disrupt the operation of the turbine, the consequences of which are not predicted. Therefore, this system should be subject to the same minimum-security requirements and measures as the system mentioned in figure 6.2.

Another case of this investigation, where an identification system was applied, but we were connected to the device successfully (figure 6.4). As I made research of PLC and opened ports, I found on one port the device (figure 6.4). This is a 3G router (using SIM card).



CP 343-1 CX10

**General:**

Station name: SIMATIC 300(1)

Module name: CP 343-1 Lean

Module type: CP 343-1 Lean

**Status:**

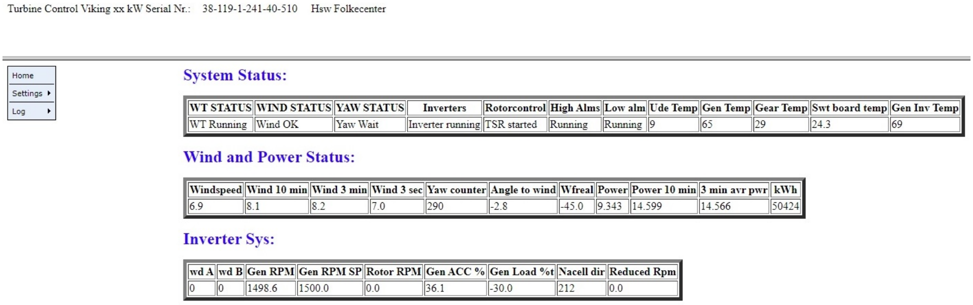
Operating state: RUN

**Module access protection:**

Protection level: Not locked

Cause: Configured protection level

**Figure 6.2:** Connection to Siemens S7 SIMATIC 300 [SHO]



Turbine Control Viking xx kW Serial Nr.: 38-119-1-241-40-510 Hsw Folkecenter

System Status:

| WT STATUS | WIND STATUS | YAW STATUS | Inverters | Rotorcontrol | High Alms | Low alm | Ude Temp | Gen Temp | Gear Temp | Swt board temp | Gen Inv Temp |
|---|---|---|---|---|---|---|---|---|---|---|---|
| WT Running | Wind OK | Yaw Wait | Inverter running | TSR started | Running | Running | 9 | 65 | 29 | 24.3 | 69 |

Wind and Power Status:

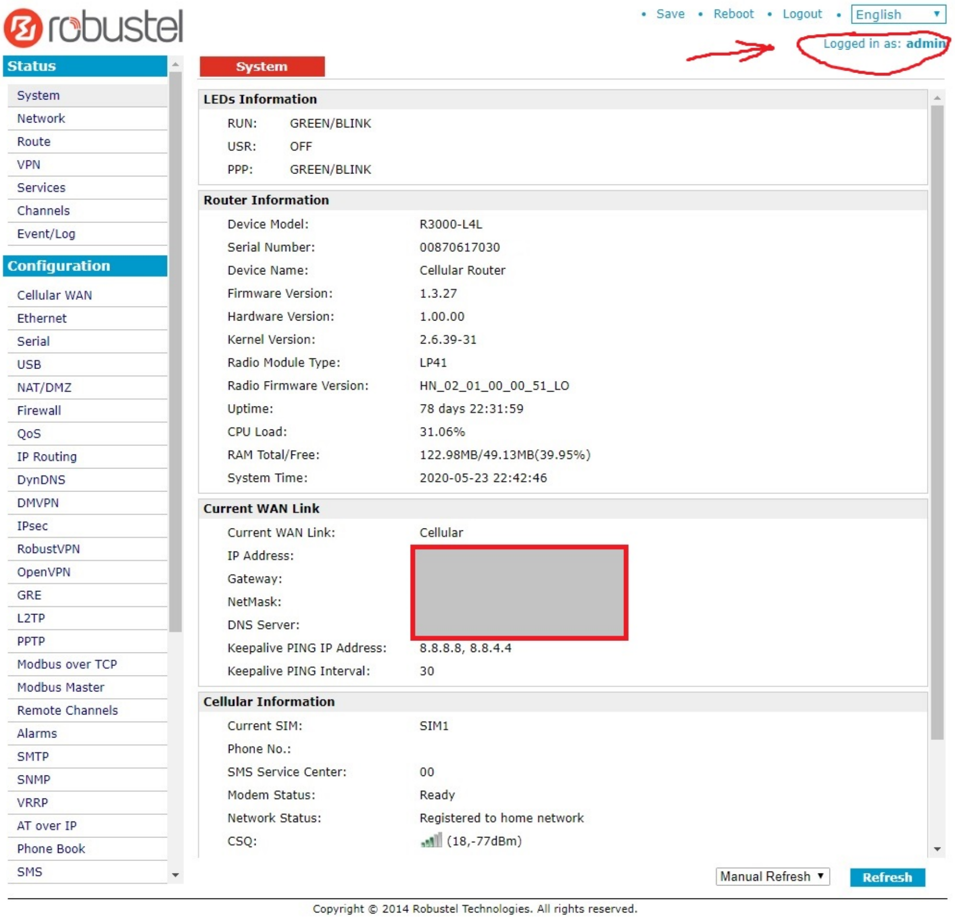
| Windspeed | Wind 10 min | Wind 3 min | Wind 3 sec | Yaw counter | Angle to wind | Wfreal | Power | Power 10 min | 3 min avr pwr | kWh |
|---|---|---|---|---|---|---|---|---|---|---|
| 6.9 | 8.1 | 8.2 | 7.0 | 290 | -2.8 | -45.0 | 9.343 | 14.599 | 14.566 | 50424 |

Inverter Sys:

| wd A | wd B | Gen RPM | Gen RPM SP | Rotor RPM | Gen ACC % | Gen Load %t | Nacell dir | Reduced Rpm |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1498.6 | 1500.0 | 0.0 | 36.1 | -30.0 | 212 | 0.0 |

**Figure 6.3:** Connection to turbine control system [SHO]

Note in figure 6.4 that we are logged in as an administrator. Although authentication was used here, to device we were logged in using the default password. This is a fairly common case, where the system owner uses the device without changing the factory password. As in the previous examples, the port is also open here. Although an identification system was in place, the username and password were not changed and left at the factory. After logging in to this system, a hacker can change the username, Wi-Fi password, read incoming SMS messages and use the available information about users to perform further hacking actions. In this way, users could not only be left without access to the Internet, but also lose their own personal information.



Logged in as: admin

System

**LEDs Information**

RUN: GREEN/BLINK
USR: OFF
PPP: GREEN/BLINK

**Router Information**

Device Model: R3000-L4L
Serial Number: 00870617030
Device Name: Cellular Router
Firmware Version: 1.3.27
Hardware Version: 1.00.00
Kernel Version: 2.6.39-31
Radio Module Type: LP41
Radio Firmware Version: HN_02_01_00_00_51_LO
Uptime: 78 days 22:31:59
CPU Load: 31.06%
RAM Total/Free: 122.98MB/49.13MB(39.95%)
System Time: 2020-05-23 22:42:46

**Current WAN Link**

Current WAN Link: Cellular
IP Address: [redacted]
Gateway:
NetMask:
DNS Server:
Keepalive PING IP Address: 8.8.8.8, 8.8.4.4
Keepalive PING Interval: 30

**Cellular Information**

Current SIM: SIM1
Phone No.:
SMS Service Center: 00
Modem Status: Ready
Network Status: Registered to home network
CSQ: (18,-77dBm)

Copyright © 2014 Robustel Technologies. All rights reserved.

**Figure 6.4:** Successfully logged to the device as administrator [SHO]

The following minimum steps should be taken to solve this problem:

- The port should be closed;
- The device administrator name and password should be changed to meet the requirements mentioned in the previous chapter of this paper.

## 6.2 Conclusion of practical part

In conclusion to chapter 6, we can refer back to previous sections and to look thru type of violations we have discovered:

1. Found PLCs with open ports and info about PLCs, which is publicly available;
2. Monitoring systems with info is available without authentication;
3. Found Internet device with default password.

To summarize this investigation, it can be said that the possible violations, mentioned in the third chapter of the project, are not only theoretical. This practical part showed that they really do exist and that information security specialists should do their work here. It is projected that there will be 21 billion devices on the Internet in 2025, compared to 4.7 billion in 2016 [Ger]. In this case more information security specialists will be needed to protect these devices.

# Chapter 7 CONCLUSION

Information is undoubtedly one of the most valuable resources of the enterprise. It is necessary at the decision-making stage, when implementing the tasks of economic activity and management. It is through the use and analysis of the necessary information that the manager prepares relevant reports, proposals for the final development and adoption of management decisions. Obviously, before you start working with information, you need to structure it and prepare it for use, because at the initial stage an enterprise interacts most often with raw information. The problem of transferring information into a state of usefulness is solved by the information system operating at the enterprise.

Information security rules play a key role in securing systems and networks. Thoughtful, implemented and implemented information security rules will help to feel the difference between security hints and an organized security system, that works effectively.

Despite the fact that the policy does not answer the question of how the technological goals should be achieved, nevertheless, having properly determined what needs to be secured, we thereby ensure that the process is properly managed. The security rules describe what should be protected and what restrictions are imposed on the management. Despite the fact that they do not discuss either the nomenclature of the manufactured product or production cycles, safety rules will help to better navigate both, when choosing a product and when choosing ways to develop a company. Implementation of policy requirements will provide higher security for the entire system.

In this thesis we got to know how industrial control systems work, looked at the eyes of a hacker, how the hacking is carried out, mentioned the main problems and risks of information security, mentioned several systems as possible solutions and concluded that the measures and means, discussed in this work, are not enough. In particular, information assets are at risk, which can be transferred in the form of files or a conversation between the head office and company branches, which does not guarantee their reliable protection.

It is proposed to use one of the DLP systems - Garda Enterprise DLP system (other DLP systems also good solutions) as the main software package, which will make it possible to organize a reliable system for protecting information from intrusions and leaks. The proposed set of measures will bring information security of the processed and transmitted information to a new level.

Further improvement of the information security system is supposed to be developed in the direction of convergence of various areas of information security, in particular in the following areas:

- Continuous modernization of the information security system;
- Stricter requirements for staff;
- Strict implementation and monitoring of the developed security policy;
- Creation of the concept of inevitable liability for violation of the requirements of the security policy of employees of the enterprise;
- Introduction of modern software systems for information security.

# References

[154] GOST R ISO / IEC 15408-1-2002. **"Information technology. Methods and means of support. Criteria for assessing the security of information technology. Part 1. Introduction and general model"**. 2002.

[270] GOST R ISO / IEC 27001-2006. **"Methods and means of security. Information Security Management Systems"**. 2006.

[A.Aa] Denisova A.A. **"The basics of cryptography"**. Yurayt, 2017, 289 p.

[A.Ab] Efimov A.A. **"Data protection"**. Knorus, 2017, 594 p.

[AD] Novak Miroslav Astels David, Miller Granville. **"Practical Guide to Extreme Programming"**. Williams Publishing House, 2008, 320 p.

[A.E] Isamidinov A.E. **"Protection of trade secrets in the field of labor relations"**. Lenand, 2017, 120 p.

[A.O] Chefranova A.O. **"ViPNet Information Protection System. Lecture course"**. DMK-Press, 2015, 392 p.

[ASa] K.A. Shcheglov A.J. Shcheglov. **"COMPUTER SECURITY. New Technologies, Methods, and Means of Additional Protection of Information from Unauthorized Access"**. Collection of articles, SPB, 2015.

[A.Sb] Minzov A.S. **"Methodology for the application of terms and definitions in the field of information, economic and integrated business security"**. Research Institute of Geosystems, 2011, 84 p.

[A.Va] Malyuk A.V. **"Analysis and forecasting of the need for information security specialists"**. Hot Line - Telecom, 2017, 214 p.

[A.Vb] Polyakov A.V. **"Oracle security through the eyes of the auditor. Attack and defense"**. DMK Press, 2017, 336 p.

[emp] Symantec employee. **What is the Difference Between Black, White and Grey Hat Hackers?** https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hacke html. Accessed: 2019.

[EN] Popov I.A. Emelyanova N.A., Partyka T.V. **"Protection of information in a personal computer. Tutorial"**. Forum, Infra-M, 2015, 368 p.

[FST] FSTEC. **"Methodology for determining the actual threats to the security of personal data during their processing in personal data information systems"**. FSTEC, November 16, 2009.

[Gal] Cesare Gallotti. **"Information security: risk assessment, management systems, the ISO/IEC 27001 standard"**. Lulu, 2019, 354 p.

[Ger] Joe Gervais. **"The future of IoT: 10 predictions about the Internet of Things"**. https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html. Accessed: 2020.

[G.G] Buzov G.G. **„Protection of limited access information from leakage through technical channels“**. Hot Line - Telecom, 2017, 594 p.

[GL] DNV GL. **"Cyber security services"**. https://www.dnvgl.com/services/cyber-security-services-127179. Accessed: 2019.

[GS] Cherepnev M.A. Gashkov S.B., Primenko E.A. **"Cryptographic methods of information protection"**. Academy, 2010, 304 p.

[HC] Hongbiao Gao-Jingde Cheng Huilin Chen, Da Bao. **"A Security Evaluation and Certification Management Database Based on ISO/IEC Standards"**. https://ieeexplore.ieee.org/document/7820455. Accessed: 16.12.2016.

[inf] Search inform. **"Information Security Threats"**. https://searchinform.com/infosec-blog/2019/08/17/fundamentals-of-is-data-protection/information-security-threats/. Accessed: 17.05.2019.

[ISA] ISACA. **"COBIT 5 for Information Security"**. ISACA, 2012, 220 p.

[J.S] Sergeeva J.S. **"Information Security. Lecture notes"**. A-Prior, 2011, 128 p.

[KN] Kondrashova T.V. Kunyaev N.N., Demushkin A.A. **"Confidential record keeping and secure electronic document management"**. Logos, 2017, 500 p.

[Lai] Christopher Laing. **"Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection: Approaches for Threat Protection"**. IGI Global, 2012, 450 p.

[Lawa] Federal Law. **"Information, Information Technologies and the Protection of Information"**. July 27, 2006 No. 149-FZ, amended by: July 27, 2010, April 6, July 21, 2011, July 28, 2012, Ap

[Lawb] Federal Law. **"On Personal Data"**. July 27, 2006 No. 152-FZ, amended on July 21, 2017.

[LF] Ronald Dodge Lynn Futcher. **"Fifth World Conference on Information Security Education"**. Springer, 2007, 148 p.

[M.Aa] Adamenko M.A. **"Fundamentals of classical cryptology. Secrets of ciphers and codes"**. DMK Press, 2012, 256 p.

[M.Ab] Metsaputyan M.A. **"Protection of confidential information. Tutorial"**. DROFA, 2017, 256 p.

[M.Ac] Vus M.A. **"Informatics: introduction to information security"**. SPb., 2012, 156 p.

[MH] J. Viega M. Howard, D. Leblanc. **"24 mortal sin computer security"**. Peter, 2010, 400 p.

[MV] Skhirtladze A.V. Melnikov V.V., Kupriyanov A.A. **Data protection. Textbook"**. Educational and Publishing Center "Academy", 2017, 304 p.

[NJ] McLachen D. Novak J., Northcutt S. **"How to detect network intrusion. Handbook of a systems analysis specialist"**. Lori, 2012, 384 p.

[N.V] Grishina N.V. **"Integrated information protection system at the enterprise"**. Forum, 2010, 240 p.

[oEC] Council of Europe Convention. **"Protection of Individuals with regard to Automatic Processing of Personal Data"**.

[P.A] Horev P.A. **"Hardware and software information security. Tutorial"**. Forum, Infra-M, 2015, 352 p.

[Pos] Howard Poston. **"What is Black Box, Grey Box, and White Box Penetration Testing?"**. https://resources.infosecinstitute.com/what-are-black-box-grey-box-and-white-box-penetration-testing/#gref. Accessed: 2019-01-19.

[Pou] Don Poulton. **"MCTS 70-642 Cert Guide: Windows Server 2008 Network Infrastructure, Configuring"**. Pearson Education, 2012, 866 p.

[RB] Fionov A.N. Ryabko B.J. **"Cryptographic methods of information protection"**. Hot Line - Telecom, 2012, 230 p.

[SHO] SHODAN. **"Shodan is the world's first search engine for Internet-connected devices"**. https://www.shodan.io/. Accessed: 20.05.2020.

[Sta] Standard. **"Ensuring Information Security of Organizations of the Banking System. General Provisions"**. adopted and enforced by order of the Central Bank, November 18, 2004 N P-609.

[SVa] Kurbatov V.A. Skiba V.J. **"Guidelines for protection against internal threats to information security"**. Peter, 2011, 320 p.

[S.Vb] Vorontsova S.V. **„Information security in the banking sector. Monograph“**. Knorus, 2015, 160 p.

[Sys] Systematic. **"Securing integrated solutions"**. https://systematic.com/ins/s/cyber-security/. Accessed: 2020.

[V.Aa] Ishaynov V.A. **"Organizational and technical support of information security. Protection of confidential information. Tutorial"**. DROFA, 2017, 256 p.

[V.Ab] Serdyuk V.A. **"Organization and information protection technologies. Detection and prevention of information attacks in automated systems of enterprises"**. Higher School of Economics (State University), 2011, 576 p.

[V.F] Shangin V.F. **"Information Security"**. DMK-Press, 2017, 702 p.

[Wil] Jim Wilson. **"What Shodan Is and How to Use It Most Effectively"**. https://www.safetydetectives.com/blog/what-is-shodan-and-how-to-use-it-most-effectively/. Accessed: 17.06.2019.