Logo, company name, sunburst chart

Description automatically generated

Mauletkhanov Y. Y.

Abdubayev R.

**Building a model of security threats of credit organization information**

Diploma work

6B06301 – «Cyber Security»

**Supervisor:**

**Senior-lecturer, Kuat Beisekeyev**

Astana, 2023

**Annotation**

A thorough investigation into the model of potential risks to the information security of a financial institution is the objective of the research being conducted for this thesis. The goal of the study is to identify and investigate the potential security risks that credit institutions face, both those that originate from within the institution and those that originate from outside the institution, with a particular focus on developing risks. This study will contribute to the existing body of knowledge by identifying gaps and limits in the present understanding of security threats in financial institutions. After conducting a thorough assessment of the literature, this study will contribute to the existing body of knowledge. The objective of the study is to gather pertinent data from financial institutions by employing proper research procedures, such as observations, as part of the research process. These data will be analyzed using the appropriate analysis methodologies in order to evaluate the efficacy of the present security measures as well as the countermeasures that have been implemented by credit institutions. Using several risk assessment approaches, the study will also evaluate the potential impact as well as the likelihood of the identified security concerns. In addition, the goal of the study is to produce suggestions for credit institutions to improve their security threat model, improve their security measures and countermeasures, and successfully decrease security risks. These improvements will be made possible by the findings of the study. The purpose of the study is also to shed light on incident response and recovery tactics, such as incident management, investigations, forensic procedures, and planning for business continuity. In a broader sense, the purpose of this thesis is to make a contribution to the field of information security of credit institutions by broadening one's understanding of security threats, risk assessment, and incident response as they pertain to credit institutions. Credit institutions will receive useful information as a result of the results and suggestions of this study, which will help them improve their security architecture and safeguard their precious information assets from potential security risks.

**Keywords:** information security, financial institutions, cybersecurity, documentation

LIST OF ABBREVIATIONS AND DESIGNATIONS

ARM - automated workplace

AS - automated system

ASZI - automated system in protected execution

ISPD - Personal Data Information System

LAN - local area network

OS - operating system

PD - personal data

PMV - software and mathematical impact of software

PEMIN - side electromagnetic radiation and guidance

SAS - security analysis system

SPDS - system (subsystem) of personal data protection

SKZI - means of cryptographic protection of information

IDS - intrusion detection system

TERMS AND DEFINITIONS

**An automated system** is a system comprises of a workforce and a sophisticated set of automated tools that facilitate their operations, utilizing information technology to execute predetermined tasks.

**An automated system in protected execution (ASSI)** is an automated system is a technological implementation that executes predetermined functions in compliance with established standards and/or regulatory documents pertaining to information security.

**Attack** – targeted actions of the violator engages in deliberate and focused actions utilizing technical and/or software tools with the intention of breaching the established security parameters of the information safeguarded by the cryptographic medium or to facilitate such a breach.

**Authentication of the data sender** is a confirmation that the sender of the received data corresponds to the declared one.

**A virus (computer, software)** is an executable program code or an interpreted set of instructions that has the properties of unauthorized distribution and self–reproduction. The created duplicates of a computer virus do not always coincide with the original, but retain the ability to further spread and reproduce themselves.

**Malicious program** is a program designed to carry out unauthorized access and (or) impact on personal data or resources of the personal data information system.

**Documented (declared) software capabilities (TS)** – software functionality (TS) described in the software documentation (TS).

**Access to the operating environment of a computer (personal data information system)** – obtaining the ability to run regular commands, functions, operating system procedures (destruction, copying, moving, etc.), executable files of application programs.

**Protected information** is information that is the subject of ownership and is subject to protection in accordance with the requirements of legal documents or requirements established by the owner of the information.

**Identification** is the assignment of an identifier to the subjects and objects of access and (or) comparison of the presented identifier with the list of assigned identifiers.

**The personal data information system** is a set of personal data contained in databases and information technologies and technical means that ensure their processing.

**Confidentiality of information** is a mandatory requirement for a person who has access to certain information not to transfer such information to third parties without the consent of its owner.

**Confidentiality of personal data** is a mandatory requirement for the operator or other person who has access to personal data to prevent their dissemination without the consent of the subject of personal data or the presence of other legal grounds.

**Introduction**

Credit institutions play an essential part in the present digital age, both in terms of the management of personal consumer information and the facilitation of financial transactions. Because of the growing reliance on technology, there is an ever-increasing requirement for stringent security measures to protect this valuable data from a variety of security risks. Because any breach or compromise of a credit institution's information security can result in significant monetary losses, harm to reputation, and a loss of client trust, maintaining the integrity of that information's security is of the utmost significance. As a result, it is essential to construct a thorough information security threat model that is tailored specifically to the data of a credit institution.

The objective of this thesis is to investigate the nuances of the threat model used for information security at a financial institution, with a particular focus on locating, comprehending, and eliminating potential dangers. This research is to provide a contribution to the current body of knowledge regarding information security in credit institutions by reviewing the previously published literature, carrying out empirical studies, and performing an in-depth analysis of real-life cases. Large amounts of sensitive data are processed by credit institutions such as banks, credit unions, and other financial institutions. This data includes client financial statements, personal information, and transaction details. Because they contain such a wealth of information, they are likely to be attacked by cybercriminals who are looking to take advantage of security flaws and gain unauthorized access. As a consequence of this, financial institutions face a diverse array of security risks, both internal and external, that have the potential to dramatically impact their operations as well as the faith that their customers and other stakeholders place in them.

Threats to the safety of financial institutions come in a variety of forms and are always undergoing further development. Employee malfeasance, purposeful attacks by insiders, or even unintentional behaviors that affect data security can all be considered to be internal dangers. Hacking, phishing assaults, social engineering, malware, and other forms of malware are all examples of external dangers. The rapid advancement of technology has resulted in the emergence of new dangers, such as ransomware and assaults that make use of artificial intelligence, which present significant challenges for the information security of financial institutions. In order to devise solutions that are successful against these dangers, it is of the utmost importance to have a complete understanding of and investigation into them. Existing security measures that are implemented by credit institutions, such as firewalls, encryption, access control, and intrusion detection systems, are designed to provide protection against potential attacks. Nevertheless, it is necessary to assess the efficiency of these measures and locate any openings or weaknesses that may be present in the security infrastructure. This study seeks to provide insight into areas where changes may be made to establish a more dependable information security system for a credit institution. This will be accomplished by conducting an in-depth analysis of the various security measures that are already in place. Credit institutions are required to perform exhaustive risk assessments in order to successfully limit the dangers to the institution's security. Methods of risk assessment, such as qualitative and quantitative approaches, play an important part in the process of finding, analyzing, and ranking security threats according to the potential damage they could cause and the likelihood that they will occur. Credit institutions are in a better position to efficiently allocate resources and put in place security measures that are targeted when they have conducted a full risk assessment and identified the most important threats. Credit institutions must to be ready to effectively respond to any security issues, in addition to taking preventative safety precautions. The ability to detect security breaches, bring them under control, and recover from their effects requires thorough incident response planning and administration, as well as investigative and forensic tools. In addition, the creation of business continuity and disaster recovery strategies assures that financial institutions will be able to promptly restart their operations and reduce the impact of any security breaches that may occur.

Credit institutions will have access to valuable information as a result of this study's findings and recommendations, which will help them improve their security threat model. This study intends to assist credit institutions in strengthening their security infrastructure by identifying vulnerabilities, recommending changes to security measures and countermeasures, as well as offering techniques for mitigation of those weaknesses. In the end, this will enable them to secure their important information assets, continue to keep the trust of their customers, and ensure the integrity and stability of the ecosystem in which the financial system operates. In the course of this research, a strategy that is methodical and stringent will be utilized. This will include conducting an exhaustive evaluation of the available research on security threat models and the information security of credit institutions. This study attempts to enhance past knowledge and contribute new ideas to the subject by analyzing previous research, locating gaps and limitations in the current body of literature, and defining those gaps and limitations. The study will identify and categorize potential security vulnerabilities that credit institutions face, taking both internal and external considerations into consideration. Credit institutions are able to design focused strategies and efficiently deploy resources to decrease risks when they have a comprehensive grasp of the type and characteristics of the dangers they face. During the course of the investigation, a particular focus will be placed on new dangers such as ransomware and assaults that make use of artificial intelligence. These types of attacks generate particular challenges that call for preventative actions to be taken. This study will give recommendations for upgrading the security architecture of financial institutions based on an assessment of the existing security measures and countermeasures. These recommendations might include things like technological advancements, employee training and awareness initiatives, a review of policies and processes, and co-operation with industry experts and regulators. The purpose of this project is to offer solutions that are actionable and can be put into place to increase the safety of financial institutions. It is essential to be aware that this study has a number of shortcomings that need to be addressed. The scope of the study will primarily concentrate on financial institutions, and it is possible that the findings will not be directly transferable to other industries. In addition, the research will be carried out over a specific amount of time, and it is possible that it will not investigate newly surfaced dangers or gaps in security that become apparent after the conclusion of the study. In spite of this, the conclusions that were reached as a consequence of this study will make a contribution to the comprehension of security threat models that are present in the information held by credit institutions, as well as provide a foundation for more research in this field.

In conclusion, it should be emphasized that the model of risks to the security of information of a credit institution is the most essential topic of research. The purpose of this thesis study is to close this knowledge gap by performing an in-depth analysis of the security risks that credit institutions are up against, assessing the efficiency of the security measures that are now in place, determining the level of risk, and offering suggestions for ways to make improvements. This research intends to contribute to the preservation of personal information, the maintenance of consumer trust, and the general stability of the financial ecosystem by strengthening the security of credit institutions.

**Methodology**

The study will employ a research methodology known as a mixed-method approach, which combines qualitative and quantitative approaches. Using this technique, you are able to obtain a thorough understanding of the model of threats to the security of information held by a credit institution. This understanding encompasses both the subjective information and the objective data.

Techniques for the collecting of data:

Interviews will be conducted with key stakeholders from financial institutions, such as IT security specialists, managers, and staff. Interviews with a degree of structure will be used to collect qualitative data from respondents regarding their experiences, perceptions, and challenges in relation to potential security risks. The interviews are going to be transcribed after they have been recorded acoustically. The qualitative data that was gathered as a consequence of the interview will be subjected to a theme analysis, and this analysis will be performed on the data. During this step, you will be tasked with locating recurring themes, patterns, and connections within the data. After the generation of source codes has been completed, the next step will be to organize the codes into useful categories. Either by hand or with the use of software designed specifically for qualitative research, the analysis will be conducted to ensure its rigor and dependability.

Ethical considerations:

a. Informed consent: Participants will be given comprehensive information regarding the study, its goal, and the significance of their voluntary involvement. Before beginning the process of data collecting, we will make sure that every participant has given their informed consent. b. Anonymity and confidentiality: During the process of data processing and reporting, neither the identity of the participants nor their responses will be revealed; instead, both will be anonymized. Only the aggregated data will be supplied in order to protect the privacy of the many individuals and organizations involved.

Limitations:

a. The size of the sample: The size of the sample may be restricted due to a lack of time and resources, which may have an impact on the results' capacity to be generalized. b. Time constraints: The research will be carried out over a predetermined amount of time, which may restrict the depth and breadth of the data collected as well as the analysis done on the data. c. Credibility from an external perspective: Due to the diversity of organizational structures, security procedures, and threat landscapes, the conclusions may not be immediately applicable to all credit institutions. However, in order to make the results of the study more applicable to a wider population, we will be making an effort to pick a representative sample. Due to the fact that such documents as the threat model of credit institutions are confidential, we will not write in which organization this data was taken and which participants participated in it.

In spite of these constraints, the technique that was selected has been devised with the intention of providing a dependable and thorough understanding of the model of risks to the information security of a credit institution. The study is able to cover the complete complexity of security risks since it incorporates both qualitative and quantitative research methods. As a result, the study is able to give credit institutions with vital information that will help them enhance their level of security.

**Theoretical part**

**Description of the personal data information system in credit institutions, including a description of the information technology infrastructure.**

Personal data information system is an information system, which refers to a collection of personal data that is stored in a database. It also encompasses information technologies and technical resources that facilitate the processing of this personal data, with or without the aid of automation tools. When it comes to the collecting, storage, processing, and administration of personal data of individuals who are clients or potential customers of credit institutions, the personal data information system is an extremely important component of the whole picture. Credit institutions bear the responsibility of safeguarding personal data as custodians, and must ensure that the collection and handling of personal data obtained from customers or prospective customers is conducted in a secure and appropriate manner. The personal data information system is an essential element in credit institutions, facilitating the systematic and well-organized administration of personal data. The present system comprises a multitude of interrelated components and processes that collectively facilitate the efficient and legal management of individuals' personal information. Comprehending the complexities of this particular system is of utmost importance in upholding the privacy rights of individuals and guaranteeing adherence to pertinent data protection statutes and guidelines.

The personal data information system at financial institutions is comprised of a number of essential components, each of which serves a unique function. The first step in the process is known as "data collection," and it is the stage in which financial institutions collect personal information from customers when they open new accounts or apply for new credit products. The majority of the time, this information consists of identifying details, contact information, financial records, and employment details. When the data have been acquired, they are then stored in a safe manner in databases or other data storage systems. These systems use a variety of security methods, such as encryption and access controls, to secure the confidentiality of the data as well as its integrity.

The processing of data is an important step within the overall framework of the personal data information system. The information that is gathered is put to use by credit institutions in the process of carrying out operations such as credit evaluation, underwriting, loan disbursement, and account administration. Processing data entails making choices about creditworthiness, risk assessment, and loan management based on personal information in order to act in an educated manner. This stage is extremely important in the process of guaranteeing responsible lending practices and sustaining the financial health of the credit institution.

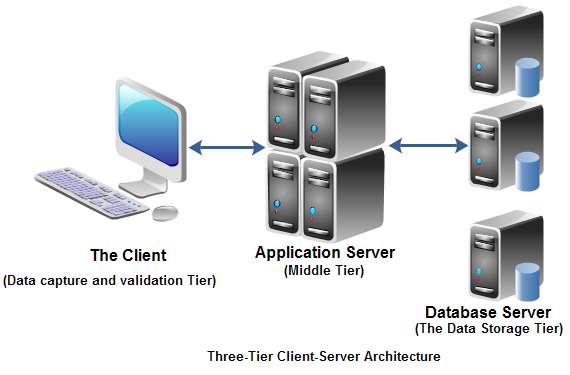
The personal data information system also includes a component that is very necessary—data retrieval. When necessary for credit-related activities, customer enquiries, regulatory compliance, or legal responsibilities, authorized persons inside the credit institution have access to and can obtain relevant personal data stored there. The implementation of access controls ensures that only authorized personnel are able to access and retrieve the data, hence preserving the confidentiality of the data and ensuring its security.

Within the context of the personal data information system, the protection of data is of the utmost significance. Credit institutions have an obligation, both legally and ethically, to preserve personal data and comply with any applicable data protection requirements, such as the General Data Protection Regulation (GDPR) or local data protection legislation. This commitment applies to both the data that the institution stores and the regulations that govern its use. In order to protect personally identifiable information from being accessed in an unauthorized manner, lost, or misused, precautions such as security audits, risk assessments, and encryption methods are taken.

In addition, financial companies that provide credit have guidelines and protocols for the storage and deletion of customer data. These policies establish the length of time personal data should be maintained, taking into consideration regulatory obligations, the requirements of the business, and the preferences of the customers. When data is no longer required, it should be disposed of in a secure manner so that it cannot be accessed by unauthorized parties or compromised.

The personal data information system in credit institutions encompasses the technological infrastructure that supports the collection, storage, processing, and management of personal data. The information technology (IT) infrastructure of credit institutions typically includes the following components: servers and databases, network infrastructure, security measures, backup and disaster recovery, data processing applications, client devices and interfaces.

1. Credit institutions use servers to store and handle enormous volumes of personal data. Databases are also used for this purpose. Databases are used to their full potential in order to effectively organize and structure the data. These servers and databases could be hosted on-premises within the credit institution's very own data centers, or they could be outsourced to third-party cloud service providers. A data bank is a repository of information on one or more subjects that is organized in database management and information architecture to make it easier to access information locally or remotely and to handle a large number of continuing enquiries over an extended period of time. Another name for a data bank is a databank. A data bank is a firm whose primary purpose is the establishment and maintenance of such a database, and the term is sometimes used to refer to such a company. The information storage and retrieval processes of a data bank can either be centralized or decentralized. However, because of the analogy with a bank of money, the majority of people use the phrase "data bank" to refer to centralized processes. A data bank may store everything from records from the financial system, such as credit card transactions, to records from the scientific community, such as readings of the world temperature, to records from the government, such as census figures, to records from the scientific community, such as readings of the global temperature, to the merchandise sold by numerous vendors. Database management systems are responsible for storing and retrieving a significant amount of data. A large amount of data is managed by banks. They can store, manipulate, and retrieve data quickly enough for both themselves and their clients using a database management system (DBMS). The example of server and database is shown in Figure 1.1



2. Network infrastructure. Within credit institutions, the network infrastructure is an essential component in playing a supporting function for the personal data information system. It covers the different pieces of hardware, software, and protocols that make it possible for the various components of the information system to communicate in a safe and dependable manner. This sub-chapter discusses the fundamental components that make up the network infrastructure in credit businesses. These routers, switches, firewalls, and other network devices are among the topics covered. In order to demonstrate the significance of the network infrastructure and its relevance to the industry as a whole, some examples of credit organizations will be offered. Credit institutions rely on a wide variety of network devices to assist with the transmission of data, guarantee the security of the network, and ensure continuous connectivity. Routers are an essential component of network infrastructure since they are responsible for forwarding data packets between various networks. They set up communication channels and figure out the most expedient pathways for the transmission of data. Routers from the Cisco ISR (Integrated Services Router) series and the Juniper Networks MX Series are two examples of the kinds of routers that are frequently utilized in credit institutions. Switches are another essential network item that enable the connecting of various devices inside a local area network (LAN), such as the one that the credit company uses. They make the exchange of data packets between devices easier and more effective, which in turn ensures that communication is both quick and dependable. In order to accommodate the enormous volume of data traffic produced by a variety of systems and client devices, credit firms frequently make use of enterprise-grade switches such as Cisco Catalyst switches and HP ProCurve switches. Firewalls are essential pieces of network security hardware that guard credit businesses against intrusions from unauthorized users and attacks carried out by criminal actors. They keep an eye on traffic coming into and going out of the network, implementing security rules to either let certain data packets through or block them, depending on the policies in place. Credit companies frequently use industry-leading firewall solutions, such as Palo Alto Networks Next-Generation Firewalls and Check Point Firewalls, to protect their network infrastructure and the sensitive data of their customers. Credit organizations utilize Virtual Private Networks, also known as VPNs, to establish secure communications across public networks like as the internet. Virtual private networks (VPNs) make use of encryption methods to construct an encrypted tunnel that enables the secure transmission of data. This is of utmost significance when connecting with foreign partners or branches, as well as for workers who are located in remote locations. In order to guarantee the safety of remote access and data transfer, credit businesses may decide to deploy virtual private network (VPN) solutions such as Cisco AnyConnect or Fortinet FortiGate.

Security Measures for Networks Credit firms are required to adopt stringent security measures for their networks in order to safeguard customers' personal information, thwart illegal access, and protect against data breaches. For the purpose of monitoring network traffic and identifying potentially harmful actions or intrusions, Intrusion Detection and Prevention Systems, abbreviated as IDPS, are utilized. IDPS solutions, like as Snort and Suricata, have the ability to detect and neutralize assaults in real time, thereby protecting the network infrastructure and preserving its integrity. Access controls and authentication techniques are absolutely necessary in order to guarantee that the network and its resources are only accessible to those who have been granted permission to do so. When it comes to enforcing secure access regulations, credit firms typically rely on strategies like as user credentials, two-factor authentication, and role-based access controls. In addition, Network Access Control (NAC) solutions, such as Cisco identification Services Engine (ISE) or Aruba ClearPass, can be utilized to enforce network security regulations and grant or restrict access depending on the user identification and compliance status of the user. In order to create a background that is grounded in the real world, let us assume a well-known credit company and the network infrastructure implementations it uses. Consider the case of ABC Bank as an illustration. The personal data information system of ABC Bank, a leading financial institution, is supported by a solid network infrastructure thanks to ABC Bank's efforts. They have ensured the reliability and efficacy of data transmission within their internal network by putting in place an infrastructure for their network that is based on Cisco technology. This infrastructure includes routers and switches. The network devices have been configured in such a way as to prioritize the flow of personally identifiable data and to offer a secure connection between the various departments and branches. ABC Bank has taken measures to safeguard their network infrastructure against unauthorized access and potential dangers by putting in place firewalls and intrusion detection and prevention systems (IDPS). They use a virtual private network (VPN) solution to set up secure connections for remote employees and external partners, thereby ensuring that data transmissions are kept confidential. Access controls and authentication techniques are set up so that secure access regulations can be enforced and sensitive information stored on their network may be kept safe. In order to keep a high degree of data security and network integrity, ABC Bank performs frequent network infrastructure updates and monitoring, as well as security audits and vulnerability assessments.

3. Financial institutions, like many other companies that deal with sensitive data in other industries, are tasked with determining the most effective means of backing up and storing financial data securely. When it comes to where data can be stored and how it can be maintained, financial institutions and other types of organizations, such as government agencies, are required to adhere to stringent criteria. As businesses move more of their information and apps to the cloud, they will probably be subject to a greater number of regulations, all of which must be adhered to in order to remain compliant.

A personal data information system in a credit company must have backups in addition to disaster recovery in order to be considered fully functional. These procedures are designed to protect the availability, integrity, and continuity of an individual's personal data in the event that the data is lost, the system fails, a natural disaster occurs, or some other type of unexpected event occurs. In this section, we will discuss the significance of backups and disaster recovery in credit organizations, as well as the essential components that are involved in both processes, and we will look at some instances of organizations that have successfully implemented effective backup and recovery systems.

The importance of backing up data and having a plan in place to recover it in the event of a disaster Credit firms rely substantially on customers' personal information to carry out their activities, such as doing credit assessments, managing loans, and managing customer relationships. The loss of personal data as a result of system failures, human errors, cyberattacks, or natural calamities can have serious repercussions for a company's finances, legal standing, and reputation. These risks can be mitigated by implementing backup and disaster recovery plans, which ensure data availability, cut down on downtime, and make it easier to recover quickly in the event that data is lost or the system is disrupted.

Backup plans: Credit businesses adopt backup plans to produce and maintain copies of personal data that may be used for restoration purposes. These copies can be created and maintained through the utilization of backup methods. These tactics include doing regular backups, storing backup data in a secure location, and performing verification steps to guarantee that data integrity is maintained. It is possible to utilize a variety of backup strategies, such as full backups (which duplicate all of the data), incremental backups (which copy only the changes that have occurred since the last backup), and differential backups (which copy the changes that have occurred since the last complete backup).

**Structural and functional characteristics**

1. Structural characteristics

2. Functional characteristics

Credit organizations possess an information system that displays clear structural-functional features, which enable effective data administration and bolster the varied activities of these establishments. The aforementioned traits comprise the arrangement of the organization, the architecture of data, and the amalgamation of software applications within the system. Comprehending these attributes is crucial in comprehending the fundamental structure that regulates the information system in credit institutions.

The framework of an information system is made up of the various components of the larger whole, which are referred to as subsystems. A system may be divided into subsystems, each of which is designated by a different property.

Regardless of the specifics of the application, an information system's overall composition can be broken down into a collection of specialized components known as subsystems. In this particular scenario, they are discussing the structural feature of classification, and the subsystems are referred to as supplying. As a result, the framework of every information system can be modeled as a collection of auxiliary subsystems, as shown in Figure 3.4.

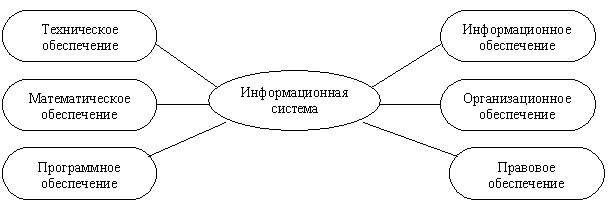


Figure 3.4. The structure of the information system as a set of supporting subsystems

Among the supporting subsystems, information, technical, mathematical, software, organizational and legal support are usually distinguished.

**Information support**

The purpose of the information support subsystem is the modern formation and delivery of reliable information for management decision-making.

Information support is a set of a unified system of classification and coding of information, unified documentation systems, schemes of information flows circulating in the organization, as well as a methodology for building databases.

*Unified documentation systems* are being created at the state, republican, sectoral and regional levels. The main goal is to ensure comparability of indicators of various spheres of social production. Standards have been developed where the requirements are set:

* to unified documentation systems;
* to unified forms of documents of various levels of management;
* to the composition and structure of the details and indicators;
* to the procedure for the implementation, maintenance and registration of unified forms of documents.

However, despite the existence of a unified documentation system, the survey of most organizations constantly reveals a whole set of typical shortcomings:

* extremely large volume of documents for manual processing;
* the same indicators are often duplicated in different documents;
* working with a large number of documents distracts specialists from solving immediate tasks;
* there are indicators that are created but not used, etc.

Therefore, the elimination of these shortcomings is one of the tasks facing the creation of information support.

*Schemes of information flows* reflect the routes of information movement and its volumes, the places of origin of primary information and the use of resultant information. By analyzing the structure of such schemes, it is possible to develop measures to improve the entire management system.

As an example of the simplest data flow scheme, we can give a scheme that reflects all the stages of passing a memo or an entry in the database about hiring an employee - from the moment of its creation to the issuance of an order for his enrollment.

The construction of information flow diagrams that allow identifying volumes of information and conducting its detailed analysis provides:

* exclusion of duplicate and unused information;
* classification and rational presentation of information.

At the same time, the issues of the relationship between the movement of information by management levels should be considered in detail. It is necessary to identify which indicators are necessary for making managerial decisions and which are not. Each performer should receive only the information that is used.

*The methodology of database construction* is based on the theoretical foundations of their design. To understand the concept of the methodology , we present its main ideas in the form of two stages that are consistently implemented in practice:

The 1st stage is a survey of all functional divisions of the company in order to:

* understand the specifics and structure of its activities;
* to build a scheme of information flows:
* to analyze the existing document management system;
* determine the information objects and the corresponding composition of the details (parameters, characteristics) describing their properties and purpose.

The 2nd stage is the construction of a conceptual information and logical data model for the sphere of activity surveyed at the 1st stage. In this model, all connections between objects and their details should be established and optimized. The information-logical model is the foundation on which the database will be created.

To create information support , it is necessary:

* a clear understanding of the goals, objectives, and functions of the entire management system of the organization;
* identification of the movement of information from the moment of its occurrence to its use at various levels of management, presented for analysis in the form of information flow diagrams,
* improvement of the document management system;
* availability and use of a classification and coding system;
* knowledge of the methodology for creating conceptual information-logical models reflecting the interrelation of information;
* creation of arrays of information on machine media, which requires the availability of modern technical support.

**Technical support**

Technical support - a set of technical means intended for the operation of an information system, as well as relevant documentation for these means and technological processes

The complex of technical means consists of:

* computers of all models;
* devices for collecting, storing, processing, transmitting and outputting information;
* data transmission devices and communication lines;
* office equipment and devices for automatic removal of information;
* operational materials, etc.

The documentation includes a preliminary selection of technical means, the organization of their operation, the technological process of data processing, technological equipment. The documentation can be divided into three groups:

* system-wide, including state and industry standards for technical support;
* specialized, containing a set of techniques for all stages of technical support development;
* normative reference used when performing calculations for technical support.

To date, there are two main forms of organization of technical support (forms of use of technical means): centralized and partially or completely decentralized. Centralized technical support is based on the use of large computers and computing centers in the information system. Decentralization of technical means involves the implementation of functional subsystems on personal computers directly at the workplace.

A promising approach should be considered, apparently, a partially decentralized approach - the organization of technical support on the basis of distributed networks consisting of personal computers and a mainframe computer for storing databases common to any functional subsystems.

**Mathematical and software support**

Mathematical and software - a set of mathematical methods, models, algorithms and programs for the implementation of the goals and objectives of an information system, as well as the normal functioning of a complex of technical means.

The means of *mathematical support* include:

* management process modeling tools;
* typical management tasks;
* methods of mathematical programming, mathematical statistics, queuing theory, etc.

The *software* includes system-wide and special software products, as well as technical documentation.

*System-wide software* includes software packages that are user-oriented and designed to solve typical information processing tasks. They serve to expand the functionality of computers, control and manage the data processing process.

*Special software* is a set of programs developed when creating a specific information system. It consists of application software packages (SPP) that implement the developed models of varying degrees of adequacy, reflecting the functioning of a real object.

Technical documentation for the development of software tools should contain a description of the tasks, an algorithmization task, an economic and mathematical model of the task, control examples.

**Organizational support**

*Organizational support* is a set of methods and means regulating the interaction of employees with technical means and among themselves in the process of developing and operating an information system.

Organizational support implements the following functions:

* analysis of the existing management system of the organization, where the IP will be used, and identification of tasks to be automated;
* preparation of tasks to be solved on a computer, including a technical task for the design of an IP and a feasibility study of its effectiveness;
* development of management decisions on the composition and structure of the organization, methods of solving problems aimed at improving the efficiency of the management system.

Organizational support is created based on the results of a pre-project survey at the 1st stage of database construction, the objectives of which you met when considering information support.

**Legal support**

*Legal support* is a set of legal norms that determine the creation, legal status and functioning of information systems, regulating the procedure for obtaining, converting and using information.

The main purpose of legal support is to strengthen the rule of law.

The structure of legal support includes laws, decrees, resolutions of state authorities, orders, instructions and other regulatory documents of ministries, departments, organizations, local authorities. In legal support, it is possible to distinguish the general part regulating the functioning of any information system, and the local part regulating the functioning of a particular system.

The legal support of the stages of the information system development includes regulations related to the contractual relationship between the developer and the customer and the legal regulation of deviations from the contract.

The legal support of the stages of the information system operation includes:

* status of the information system;
* rights, duties and responsibilities of personnel;
* legal provisions of certain types of management process;
* the procedure for creating and using information, etc.

Functional characteristics

The roles that information systems play in the world

The gathering of input data, storing that data, putting it through processing, and providing output information are all different functions that information systems perform. The functions are also responsible for controlling the flow of information and the feedback loop. There is also the possibility of open and closed systems being used.

**Input**

There are two different kinds of input in an information system:

* Detailed data are used in the creation of output, which is then saved and processed.
* Storage requires that the user provide precise instructions for the type of analysis to be performed.

The storing of data ought to be done on the most granular level that is practically possible. To prevent the loss of any vital data that could have been caused by errors, it is critical to do routine backups and compile a number of different summaries. The backups should also be kept in a location that is geographically distinct from the original data storage in order to protect them from catastrophic events like floods, fires, and other calamities that could have an effect on both the original data storage and the backup data storage.

**Processing**

A function that converts raw data into usable information is known as a process. The addition of the number of goods that are sold by a company by a variable such as the location of a store or the product or the time and date is a straightforward process that can be performed by anyone. Functions that do computations and are able to make assumptions about data that is lacking in order to create information from the data that is present are examples of more complicated processes.

**Various forms of feedback and control loops**

What happens to output after it has been processed and created is an example of a feedback and control loop. The system will keep repeating the same operations over and over again, and it will do so based on the results of the most recent loop, which will then have an effect on the data that is fed into the next loop. For instance, if a company's stock reaches 10, the company might consider purchasing more from a supplier. It's possible that the system checks the stock levels once each hour (in a loop), and if the stock level is higher than 10, the loop will continue without taking any action until the point where it drops to 10 or lower, at which point the command will be carried out and new stock will be ordered.

**Output**

In this context, there are two sorts of output: graphical and textual:

* Graphical output is typically utilized to examine data on a more comprehensive scale prior to its subsequent presentation in the form of charts, graphs, diagrams, and photographs.
* Textual output refers to information that is given on a more localized scale and can take the form of charters, text, or statistics.

**Comparing open and closed environments**

Depending on how they respond to and engage with the surroundings in which they are embedded, information systems can be classified as either open systems or closed systems:

* An open system will have full interaction with its surroundings, and it will be able to deal with any unexpected incident since it will monitor its environment, which implies that it will be able to modify its output in accordance with the specifics of the situation.
* Because components of a closed system are cut off from the outside world, they have limited opportunities to engage with their surroundings. A closed system will only engage in environmental interaction if it has been pre-planned and carefully considered, or if it is an integral element of an automated procedure. It only takes action in response to events that have occurred, and it only works when it is activated. Closed systems have no influence whatsoever on the environments to which they are exposed. A triggering event, such as payroll day, would initiate the operation of an automatic payroll calculator.

**Description of security threats**

Because of the widespread adoption of the internet and other associated technologies and systems for telecommunications, the use of these networks has given rise to a hitherto unanticipated risk for businesses and other types of organizations. These networks are susceptible to a variety of forms of infiltration and subversion. As a direct consequence of this, businesses and organizations will be put in a position where they are vulnerable to risks that impair information system security. There are many different locations, both inside and outside of an organization or company, that can pose a risk to its information systems. Each firm or organization should do an analysis to determine the sorts of risks that will be encountered and how those threats affect the security of information systems in order to protect their systems and information. Unauthorized access (including hacking and cracking), computer viruses, theft and accidents are some examples of potential dangers.

**Unauthorized Access** (also known as Hacking and Cracking). Unauthorized access to confidential data is one of the most common types of security concerns that are associated with computerized information systems. Hackers and crackers pose this threat. The most significant source of concern is unwelcome visitors, often known as hackers, who make use of cutting-edge technology in conjunction with their expertise to either break into computers that are meant to be safe or to disable them. Many times, the term "cracker" is used to refer to an individual rather than "hacker" when referring to someone who illegally gains access to an information system.

**Viruses that affect computer.** A computer virus is a type of malicious software that is purposefully developed to enter a computer without the consent or knowledge of the user. This malware also has the ability to replicate itself, which allows it to continue to spread. While some viruses do little more than replicate themselves, others can cause significant damage or severely affect the functionality of the system and its programs. Virus software can still lead to system crashes and the loss of data. The damage that a computer virus does may, in many instances, be unintentional and simply the product of poor programming. Examples of different kinds of viruses include Trojan horses and worms.

**Theft**. The loss of critical hardware, software, or data can have severe consequences on the effectiveness of a credit organizations. Theft can be broken down into three primary categories: theft of property, theft of data, and theft of an individual's identity.

**Accidents.** The majority of the harm that is done to information systems or corporate data is brought on by human error. In addition to the environment, the attitude and disposition of the employees will also have an effect, over time, on the amount of accidental misuse or damage that occurs. Errors committed by humans have a bigger influence on the integrity of information systems than do human-made dangers that are the result of malicious attacks. On the other hand, the majority of mishaps that pose substantial risks to the integrity of information systems are susceptible to mitigating factors.

Sub-topic: What kind of impact these dangers have on information systems?

1. Unauthorized Access (also known as Hacking and Cracking).

Hackers and crackers obtain illegal access by discovering flaws in the security defenses utilized by websites and computer systems. They frequently take advantage of numerous characteristics of the Internet that make it an open system that is simple to exploit.

1.1. Sniffing and Spoofing Hackers that are trying to conceal their genuine identity will frequently spoof, which means that they will misrepresent themselves by using false e-mail addresses or by impersonating as someone else. Sniffing is another technique that hackers use. Spoofing is the practice of redirecting a Web link to an address other than the one that was intended, with the site masquerade as the destination that was originally intended. Links that are supposed to lead to one side can be changed so that they take users to an entirely different website, one that is to the hacker's advantage. For instance, hackers can steal business and sensitive client information from a legitimate website by redirecting customers to a fake website that nearly identically replicates the real one. On this false website, hackers can collect and process orders, thus stealing business from the real website. While a sniffer is a type of program that monitors information that is traveling across a network, it is also considered to be an eavesdropping application. When sniffers are used for lawful purposes, they can assist in locating possible network trouble areas or criminal activities on a network. However, when sniffers are used for illegal purposes, they can be harmful and are extremely difficult to detect. Sniffer is a tool that gives hackers the ability to steal private information from anywhere on a network, such as sensitive reports, company files, and e-mail communications.

1.2. Attacks That Deny Service, Also Known as DOS: The primary objective of this assault is to bring the targeted network to its knees and force it to refuse service to users who are legally entitled to receive it. In order to bring the network to its knees, hackers will bombard a network server or a Web server with tens of thousands of phony communications or requests for services. They will install a little software known as zombies on some computers that are at an intermediate level in the networks. Whenever they want to launch an attack, they will run those programs remotely, which will cause the intermediate machines to simultaneously begin attacks.

2. Malware that affects computers

2.1. Worms are a type of virus that affects networks. They take use of vulnerabilities in operating systems and other types of software in order to replicate themselves endlessly over the Internet. This results in servers crashing, which prevents Internet users from gaining access to the Internet. Worms can corrupt data and programs, as well as impair or even stop the operation of computer networks. Worms can also spread to other computers. In the same way that a virus is built to enter data-processing programs and change or destroy the data, a worm serves the same purpose, but in contrast to a virus, it is not capable of copying itself. Worms can only affect one program at a time. There is a possibility that the repercussions of a worm attack will be just as severe as those of a virus attack. For instance, a worm program can be installed on a bank computer, and then the bank computer can be taught by the worm program to continuously transfer money to an unlawful account. The worm program will then delete itself.

2.2. Trojan Horses. In order to acquire access to a computer, a Trojan horse masquerades as a genuine program. Over the course of the last few years, there has been a discernible increase in the number of instances in which Trojans have been utilized to either sabotage business operations or acquire unauthorized access to confidential information. The majority of the Trojans that an organization will come across are designed to gather information and send periodic reports back to the owner. In most cases, a Trojan will have a key logging capability, sometimes known as a 'keystroke recorder,' which is designed to record every keystroke that is typed on a particular machine. The owner of the Trojan can collect a considerable variety of information by capturing data from the keyboard, including passwords and the contents of each and all e-mails that are sent out. The distribution of spyware and other forms of malware frequently makes use of Trojans as delivery tools. When a Trojan horse is acting as spyware, it will monitor the activities that take place on a computer. It is intended to provide the owners with control over the computer system that is the focus of the attack. The Trojan program functions, in all intents and purposes, as a remote control application, enabling the owner to control the target computer as though they were physically present and performing the activities themselves. The owner of the Trojan may sometimes make little effort to conceal the operations it is carrying out. This may result in the victim being able to observe the acts being carried out but being unable to stop them, unless they turn off the computer. The majority of the time, however, the Trojan is silent in its operation, and the victim is unaware that the applications are running on their computer, that files are being deleted, that e-mail is being sent, and so on. Trojan horses are malicious software that can delete files and data, but they also typically contain spyware and sometimes even backdoor programs. Trojans are typically hidden within software that is downloaded from either a trusted or untrusted source.

3. Theft

3.1. Theft by Physical Means: The phrase "physical theft" suggests that this type of theft involves the stealing of both hardware and software. Physical theft is not limited to computer systems alone; components are frequently targeted by criminals because of their small size and comparatively high value. It is of little value to point out that physical theft is not limited to computer systems. Theft via physical means results in the loss of confidentiality and availability and calls into question the integrity of the data that is stored on the disk.

3.2. Theft of Data: The act of stealing data typically involves creating copies of essential files without affecting the integrity of the originals in any way. This can involve stealing sensitive information and confidential data or making illegal modifications to computer records. Also included in this category is the act of altering computer records. These types of data can include sensitive correspondence, passwords, activation keys to software, and any other information that is saved on a victim's computer. On the other hand, in the event that the original files are lost or corrupted, the value of the material that has been copied will automatically grow. Because their operations frequently and substantially rely on access to corporate databases, service businesses are particularly susceptible to the theft of confidential information. It is impossible to conceive the impact that would be caused if a competitor were to obtain access to a client list that belonged to a sales organization. Both of the organizations would be placed on a footing that is substantially equivalent to one another as an instant consequence of such an event. On the other hand, in the long run, the first company would no longer have a significant advantage over its competitors and might even go out of business as a result.

3.3. Theft of Identity: An imposter commits the crime of identity theft when they impersonate another person by obtaining vital pieces of personal information, such as social security identification numbers, driver's license numbers, or credit card numbers. The information may be put to use in order to get credit, commodities, or services in the name of the victim, or it may be used in order to furnish the thief with bogus credentials. Because things can now be purchased online with no need for any personal interaction, identity thieves have found that the internet makes it much simpler for them to use stolen information. Hackers targeting websites frequently focus their attention on credit card files. In addition, websites that conduct business online are excellent resources for gathering personal information about customers, such as their names, addresses, and phone numbers. Criminals can create a new identity for themselves and start a new credit history if they have access to this information and are armed with it. Spam is a very problematic issue that is closely tied to identity theft. Sending unsolicited electronic mail or making irrelevant remarks in online discussion forums under the guise of offering a product or service is known as spam. Spammers frequently make use of zombie computers in order to send out millions of email messages without the knowledge of the users of the zombie machines.

4. The act of intentionally causing damage or disruption to something, typically for personal gain or to undermine a particular goal or objective, is commonly referred to as sabotage.

4.1. Individual sabotage refers to the deliberate actions taken by a dissatisfied employee with the intention of seeking retribution against their employer. The logic bomb is a type of malicious software that is designed to trigger at a predetermined time or in response to a particular event. It is a widely recognized illustration of how an employee can intentionally harm an organization's information systems. Typically, the logic bomb is triggered several months following the departure of the employee from the company. This phenomenon has the tendency to redirect suspicion from the employee. A widely recognized instance in the realm of computer security is referred to as a backdoor, which denotes a segment of program code that enables a user to bypass security protocols and obtain unrestricted entry to an information system. While back doors may serve legitimate purposes, such as facilitating program testing, they can also be employed as a tool for sabotage. It is noteworthy to mention that the occurrence of individual sabotage is decreasing as a result of several legislations.

4.2. Industrial sabotage is a relatively infrequent phenomenon, albeit with a few notable instances that have garnered significant media attention in recent years. The perpetration of industrial sabotage typically occurs with the aim of achieving a competitive or financial advantage. The conduct of the individuals involved in such activities is often characterized by a high degree of organization, with a focus on particular domains of a competing entity's operations, and bolstered by access to a significant pool of resources.

4.3. Inadvertent undermining of a process or system, commonly referred to as unintentional sabotage. The occurrence of sabotage does not necessarily require the presence of an intention to cause loss or damage. Consider the scenario in which an organization implements a novel information system with minimal advance notice and without adequate consultation. Employees may feel threatened by the new system and may wish to avoid making use of it. A common response could involve intentionally inputting inaccurate data as a means of undermining the credibility of the recently implemented system. In an alternative scenario, the employee may persist in performing tasks manually, asserting that this approach is more efficacious. In such instances, the foremost incentive for the employee is to protect their job security, with any harm or detriment inflicted upon the organization's information systems being a secondary consequence of this objective.

**Practical Part**

**INTRUDER MODEL**

This section defines a set of conditions and factors that increase the likelihood of breaking the security features of potential threat objects. These conditions and factors can be found further on in this section. For the purposes of this discussion, we will refer to threats as attacks. All of those who have broken the law are classified into one of two categories according on their affiliation: External violators are individuals who do not have the right to stay in the territory of the controlled zone within which the equipment of the Credit Institution is located. Internal violators, on the other hand, are individuals who do have the right to stay in the territory of the controlled zone within which the equipment of the Credit Institution is located.

**External intruder**

An individual who does not have direct access to the technical means and resources of the system that are located within the regulated zone is regarded to be an intruder who has violated the information security of the organization from the outside.

Since the amount of information that is stored and processed in a credit institution is insufficient for the possible motivation of an external violator to carry out actions aimed at information leakage through technical channels, it is assumed that an external violator cannot have an effect on the protected information through technical leakage channels. It is presumable that an unauthorized third party can only interfere with the protected information while it is being transmitted over various channels of communication.

**Internal Intruder**

The capabilities of an internal violator are heavily influenced by the restrictive factors that are active within the controlled zone. The most important of these factors is the implementation of a set of organizational and technical measures, which includes the selection, placement, and provision of high professional training of personnel. Other measures include the admission of individuals into the controlled zone as well as control over the procedure for carrying out work that is intended to prevent and suppress unauthorized access.

The access control system of the credit organization ensures the distinction of user rights to access information, software, hardware, and other resources in accordance with the information security policy that has been approved.

An internal violation can employ regular means.

The composition of the means that are available to the offender and that he can use to implement IS threats, as well as the possibilities for their use, are dependent on a wide variety of criteria. These elements include the specific organizational measures that have been put into place at the facilities, the financial capacities of violators, and their level of expertise. As a consequence of this, it is nearly difficult to conduct an objective evaluation of the make-up of the violator's arsenal of potential methods of carrying out threats in the general scenario.

Therefore, in order to create a reliable PD, it is assumed that the probable infringer possesses all of the means necessary for the implementation of threats, the capabilities of which do not exceed the capabilities of similar means of implementing threats to information containing information that does not constitute a state secret, as well as technical and software tools that process this information. This is done so in order to ensure that the probable infringer is able to carry out threats.

Concurrently, it is presumed that the offender lacks the following capabilities: means of interception in technical leakage channels;

means of influence through signal circuits (information and control interfaces of SVT); means of influencing sources and through power supply chains; means of influence through grounding circuits; means of active influence on technical means (means of irradiation); means of irradiation. Internal violators may include the following: a Security administrator (category I); an administrator of a particular subsystem or database (category II); a User (category III); a user who is external to a particular AU (category IV); a person with access to the data transmission system (category V); employees who have authorized access for official purposes to the premises where the elements are located, but do not have access rights to them (category VI); and service personnel (

It is generally accepted that individuals in category III and individuals in category VIII are in possession of the most sophisticated methods for carrying out threats.

People who fall into categories I and II are the ones who are tasked with administering the software, hardware, and databases necessary for the integration and interaction of the many different subsystems that make up. In accordance with the administrative powers that have been assigned to them, administrators have the potential to implement information security threats by making use of the opportunities for direct access to protected information that is processed and stored in, as well as to technical and software tools, including security tools that are used in specific AS. These threats can potentially be implemented by using the opportunities for direct access to protected information.

These individuals have a solid understanding of the fundamental algorithms, protocols, and applied security principles and concepts, as well as the specific subsystems in which they are implemented and used, as well as the broader system as a whole.

It is presumable that they would be able to employ conventional equipment in order to either discover vulnerabilities or carry out information security threats. Either this equipment is already present as part of the standard facilities, or it is related to something that is simple to acquire (like software obtained from external sources that are open to the public, for instance).

Persons who fall into categories I and II should be subject to a unique set of organizational and regulatory requirements due to the remarkable role they play in the process of selecting, recruiting, and appointing employees as well as exercising control over how functional activities are carried out.

Because it is presumed that only permitted persons will be included in the total number of people who fall into categories I-II, the individuals in question are not counted among the number of people who are likely to violate the regulation.

It is generally accepted that those who fall within categories III–VIII are among the most likely lawbreakers. assumptions on the information that the offender has access to regarding the targets of the threat being implemented.The following can be distinguished as the primary levels of understanding that those who violate the AU have regarding its provisions:

information about the purpose and general characteristics is considered to be general information. information obtained from operational documentation is considered to be operational information. information that supplements operational information about (for example, information from project documentation) is considered to be sensitive information.

In particular, the intruder may be in possession of the following information: data on the organization of work, the structure, and the technical, software, and hardware tools used; information about information resources, including the procedure and rules for creating, storing, and transmitting information, as well as the structure and properties of information flows; vulnerability data, including data on undocumented (undeclared) capabilities of hardware, software, and hardware tools; data on the principles and algorithms used by the system.

It is presumable that individuals in categories III and IV only have access to operational information, which is supplied through organizational measures. At the same time, those who fall under category IV do not have access to the automated information system (AIS), which means they do not have a password, authentication information, or key information for the system.

It is presumed that category V persons possess, in whole or in part, sensitive and operational information about the information transmission system as well as general information about AIS that makes use of this information transmission system. This general information is provided by organizational measures. At the same time, individuals who fall under category V do not have access to the password or login credentials required to utilize the AIS.

It is presumed that those in categories VI and VII do not have more knowledge than those in category V. This is because category V is the lowest possible level.

It is presumed that category VIII individuals have access to sensitive information and are functionally oriented towards AS. This information may include details regarding the vulnerabilities of both hardware and software. During the time when category VIII individuals are processing protected information utilizing GIS technical and software tools, organizational measures are designed to prevent those individuals from gaining access to those tools.

As a result, individuals that fall into categories III and VIII are the ones with the greatest information.

The degree to which the offender is aware of their actions relies on a variety of circumstances, including the particular organizational measures that have been put into place as well as the competency of the violators. As a result, it is nearly difficult to conduct an objective assessment of the amount of knowledge possessed by a potential infringer in the general case.

In connection with the previous, and in order to produce a certain degree of safety margin, it is assumed that the likely violators have access to all of the information required for the preparation and execution of threats, with the exception of information to which the violator is denied access due to the information protection system. This is done in order to produce a certain degree of safety margin. For instance, a password, authentication information, and key information are all examples of this type of data.

Assumptions made regarding the ways by which the infringer is able to carry out threats include the following: hardware components of PD protection; freely available hardware and software;

**Violators according to the threat database maintained by the Russian Federal Security Service (FSTEC)**

In addition, the threat database of the Russian Federal Service for Supervision of Economic and Technical Cooperation (FSTEC) has identified three categories of external and domestic violators: those with low potential, those with medium potential, and those with high potential.

Infringers with low potential have the option to collect knowledge about the vulnerabilities of particular components of the information system that has been disclosed in sources that are accessible to the public. In addition, those who violate this policy have the opportunity to obtain information about methods and means of implementing information security threats (computer attacks) that has been published in sources that are accessible to the general public, and/or they have the ability to independently create methods and means of implementing attacks and implementing attacks on the information system.

All of the capabilities of offenders with low potential are also available to violators with medium potential. A person using this sort of information system should be aware of the information protection procedures that are implemented in the system. They have the option to gather information about the vulnerabilities of particular components of the information system by doing code analysis of application software and individual software components of system-wide software. This can be done by using software tools that are publicly available. They are able to get information regarding the structural and functional properties and aspects of the information system's operation.

Infringers with a high potential are capable of committing all of the same offenses as infringers with a low or medium potential. They are able to conduct unauthorized access from dedicated communication networks (departmental or corporate) to which physical access is accessible and which are not safeguarded by organizational procedures. They have the ability to get access to the information system's chipset software (firmware), system and application software, telecommunications equipment, and other software and hardware in order to purposefully introduce vulnerabilities or insert bookmarks into those components of the system. They have a solid understanding of the information security precautions taken in the information system, as well as the algorithms, hardware, and software utilized in the information system. They have the chance to collect information about vulnerabilities by carrying out specialist research (often with the participation of specialized scientific groups) and making use of tools for software analysis that have been designed specifically for them. They have the ability to create methods and means of implementing threats to information security with the involvement of specialized scientific organizations and the implementation of threats using specially developed tools, including those that provide covert penetration into the information system and influence over it. They also have the opportunity to implement threats using specially developed tools. They are able to devise unique technical ways for getting information (influencing information or technical means), which can then propagate in the form of physical fields or phenomena. They are also able to exploit these unique technical means.

**Initial security level**

The first thing to determine is the global parameter – the level of initial security. It is global because it is defined once and does not change from threat to threat.

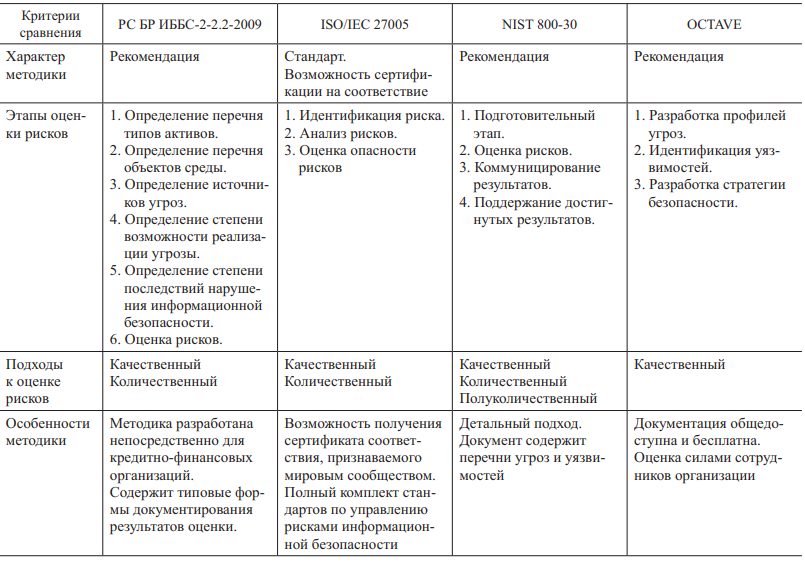
To determine the level of initial security (aka the initial security coefficient Y1), you need to select one of the values that is most suitable for your system for seven indicators.

List of characteristics and their values:

|  |  |  |  |
| --- | --- | --- | --- |
| technical and operational characteristics of ISPD | security level | | |
| high | medium | low |
| 1. by territorial placement: | | | |
| distributed ISPD, which covers several regions, territories, districts or the state as a whole | - | - | + |
| urban ISPD, covering no more than one locality (city, village) | - | - | + |
| corporate distributed ISPD, covering many divisions of one organization | - | + | - |
| local (campus) ISPD, deployed within one building | - | + | - |
| local ISPD, deployed within one building | + | - | - |
| 2. by the presence of a connection to public communication networks: | | | |
| ISPD having multipoint access to the public communication network ISPD having single-point | - | - | + |
| access to the public communication | - | + | - |
| network ISPD physically separated from the public network | + | - | - |
| 3. for embedded (legal) operations with personal data database records: | | | |
| read, search | + | - | - |
| write, delete, sort | - | + | - |
| modify, transfer | - | - | + |
| 4. on the differentiation of access to personal data: | | | |
| ISPD, to which the employees of the organization that is the owner of ISPD have access, or the subject | - | + | - |
| of the ISPD pd, to which all employees of the organization that is the owner of ISPD have access | - | - | + |
| with open access | - | - | + |
| 5. by the presence of connections with other pd databases of other ISPD: | | | |
| an integrated ISPD (organization) uses several ISPD pd databases, while the organization is not the owner of all the pd databases used) | - | - | + |
| ISPD, which uses one pd database belonging to the organization that owns this ISPD | + | - | - |
| 6. by the level of generalization (depersonalization) of pd: | | | |
| ISPD, in which the data provided to the user is depersonalized (at the level of the organization, industry, region, region, etc.) | + | - | - |
| ISPD, in which the data is depersonalized only when transferred to other organizations and is not depersonalized when provided to the user in | - | + | - |
| the ISPD organization, in which the data provided to the user is not depersonalized (i.e. there is information that allows identify the pd subject) | - | - | + |
| 7. according to the volume of PD, which are provided to third-party ISPD users without pre-processing | | | |
| ISPD, providing the entire database with | - | - | + |
| ISPD pd, providing part | - | + | - |
| of ISPD pd, not providing any information | + | - | - |

Each value represents either a high, medium, or low level of security respectively. The percentages that we acquired for indicators with varying values are taken into consideration. Forget about a high level of initial security being provided, because it will not be the case. If both "high" and "medium" scored 70% or above, then we find the average level of initial security (Y1 = 5), and if they did not, then we determine the low level of initial security (Y1 = 10).

**Danger of threats**

****

"Determining the consequences of violating information security properties (danger of threats)" is the name of this part in the template. They referred to it in that manner because, in reality, according to the definition of the danger of threats, this is the definition of consequences. However, when agreeing on the threat model, the inspectors may not draw this parallel; consequently, they write a comment because the "definition of consequences" should be included in the threat model.

Therefore, the danger posed by threats can range from low to medium to high depending on the severity of the negative outcomes that accompany the realization of the threat. These outcomes can include minor negative, simply negative, or major negative outcomes.

The danger posed by threats is a topic of frequent debate among the experts in this area. They frequently debate whether or not the danger should be determined once and then remain constant for all threats. This is not required by the approach, therefore you are free to perform both of these things. Our method takes a middle ground: we assess the level of risk posed by threats based on whether or not a particular threat compromises the confidentiality, availability, or integrity of the information being threatened.

According to our line of reasoning, the negative repercussions do not depend on the approach that was taken to violate the confidentiality, integrity, and accessibility of the information. For instance, if your personal information were to get exposed in a database, it probably wouldn't make a difference to you whether it was due to SQL injection or the intruder's physical access to the server (the financial motivations of the cybercriminal are irrelevant). As a result, we establish what we call three "threat hazards" for compromising the integrity, confidentiality, and accessibility of the information. Although they may frequently coincide, it is still best to do independent analyses of each of them in the threat model. To our good fortune, the database entry for each threat includes a description of the features that have been breached.

**Exclusion of dangers that are deemed "unnecessary"**

Next, in order to swiftly eliminate any unneeded threats, we will create a sign that includes a list of the threats that will not be tolerated as well as an explanation of why we will not tolerate them.

The following is an example of what the template provides:

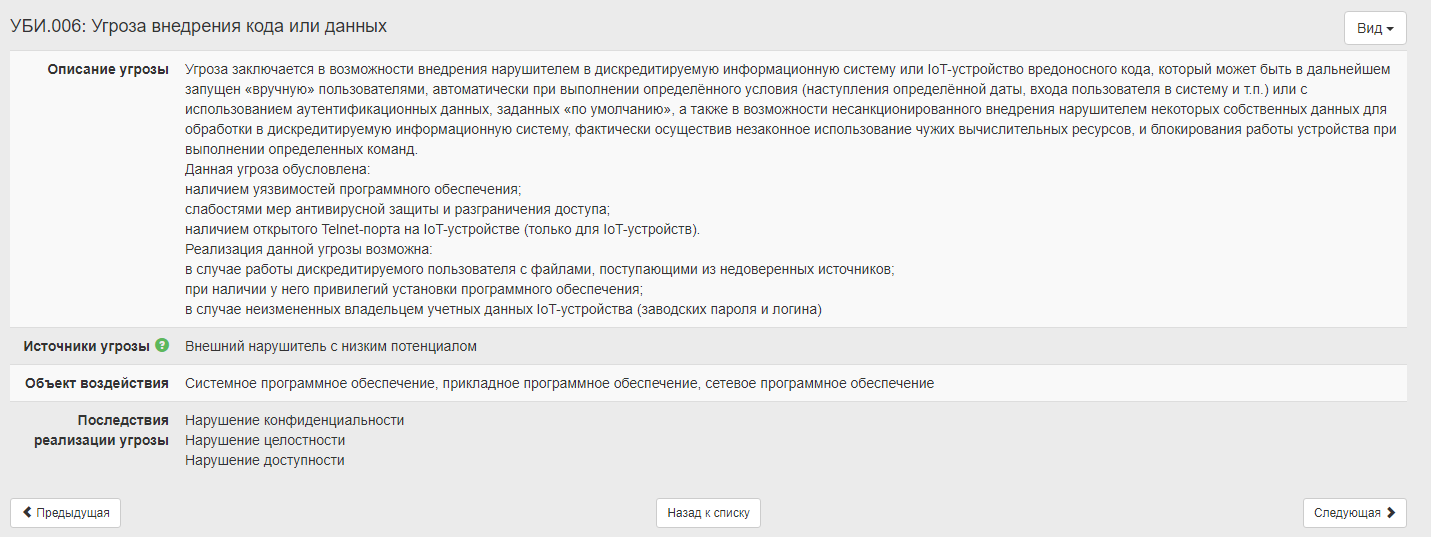
exclusion of threats associated with grid systems, supercomputers, and large amounts of data; exclusion of threats associated with virtualization; exclusion of threats associated with the use of wireless communication networks; exclusion of threats associated with the use of cloud services; exclusion of threats to the automated control system; exclusion of threats associated with the use of mobile devices; exclusion of threats the implementation of which is only possible by a violator with a high potential.

On the final point, you need to clarify a couple of points as follows: if you have identified a violator with low potential, then threats that can be carried out by violators with medium and high potential are excluded here; the only threats that are excluded are the remaining threats that were not excluded in the previous paragraphs; Pay attention to the fact that the database could specify distinct potentials for different kinds of risks to internal and external violators.

**Detailed explanation of the dangers**

The following is a table that will describe the potential dangers that have not been ruled out. Yes, in this case it is required to copy and paste the information from the database. This is because the threat model should have a "description of threats," and removing the identifiers will not accomplish the desired result. Let's have a look at the contents of this table.

Everything is made very obvious here, including the threat identity obtained from the database and the numerical order of the numbers. A text block is taken from the database and shown as the "threat description" and "method of threat implementation" columns. In the first column, just before the sentence that begins "The threat is possible...", we insert the text. The second section will cover everything else. The split can be explained once more by referring to the criterion stated in regulatory papers, which states that the threat model must contain "ways to implement the threat." When coming to an agreement, this will help to eliminate the need for further inquiries.



The probable internal and external violators are listed in the following columns of the tables. We have already compared the numbers 1, 2, and 3 to the high, medium, and low potentials, respectively, in order to make the table more condensed and to provide more room for text blocks. We insert a dash in the column for the potential if the database does not provide it.

The information for the column labeled "Objects of influence" comes from the database as well.

The column labeled "Violated properties" had its K, C, and D categories (confidentiality, integrity, and accessibility) changed to letters for the same reason as the column labeled "Violators" had its letters changed.

And the final two columns are labeled "Prerequisites" and "Justification for the absence of prerequisites." The first step is the beginning of calculating the coefficient Y2, which is also the likelihood that the danger will be realized. This probability, in turn, is decided by the presence of requirements for the threat to be realized and by taking actions to eliminate the threat. The first step is the beginning of finding the probability that the threat will be realized.

**Assessing the likelihood that a threat will materialize**

The frequency of threat realization, also known as the likelihood of threat realization, is an indication that is characterized by how likely it is to implement a particular threat to the safety of PD for a given ISPD given the preexisting conditions of the situation. This indicator is determined by specialists. There are four different levels of verbal gradation for this indicator:

unlikely: there are no objective prerequisites for the threat (for example, the threat of theft of information carriers by persons who do not have legal access to the premises where the latter are stored); low probability: there are objective prerequisites for the realization of the threat, but the measures taken significantly complicate its implementation (for example, appropriate means of information protection have been used); average probability: objective prerequisites are present but the implementation of the threat is significantly complicated (for example, appropriate means of information protection have been used); average probability: there are objective prerequisite

In the process of compiling a list of current threats to the security of PD, a numerical coefficient is assigned to each gradation of the probability of a threat. These numerical coefficients are as follows: 0 for an unlikely threat; 2 for a low probability of threat; 5 for the average probability of a threat; and 10 for a high probability of a threat.

**A rundown of the most pressing dangers**

To be more specific, the final table contains a list of threats that are now active as well as threats that are no longer relevant, as well as a summary of the remaining parameters that are used to assess whether or not they are relevant. There are no potential dangers that do not have any qualifications; nonetheless, even among the remaining potential dangers, depending on how the coefficients are calculated, some of the potential dangers could be disregarded as unimportant.

The following parameters were omitted on purpose from the previously presented table:

Y1 is a global parameter, and because of this, we just keep track of it in our heads;

prerequisites: in the final table, we only have threats that have prerequisites, therefore this column does not make any sense.

Let's spend a little bit of time going through the columns. Everything is quite evident in this situation, including the fact that the danger is already just in the form of an identity and the order of the numbers.

"Measures have been taken"—we assess by "expert" whether steps have been taken to neutralize this threat (by the way, another trick of the approach is that if measures are "taken," then the threat may still remain relevant). "Measures have been taken"—we determine by "expert" whether measures have been taken to neutralize this threat. There are three possible outcomes: accepted; acceptable, but insufficient; and not accepted (+, +-, — correspondingly). Accepted is the default outcome.

After taking into account the fact that there are conditions for the threat, the probability coefficient, denoted by Y2, has been calculated; the question now is how to decide whether or not it will be higher under the spoiler.

The next column is the Y factor, which represents the possibility of the threat. Y is determined by using the straightforward formula Y = (Y1+Y2)/20.

The Y coefficient can be thought of as the linguistic equivalent of the potential of implementation. The following is how it is defined depending on the value of the numbers:

if 0< Y < 0.3, then the possibility of implementing the threat is considered low;

if 0.3< Y < 0.6, then the possibility of threat realization is recognized as average;

if 0.6 < Y < 0.8, then the possibility of threat realization is recognized as high;

if 0.8 < Y, then the possibility of implementing the threat is recognized as very high.

|  |  |  |  |
| --- | --- | --- | --- |
| The possibility of implementing the threat |  |  |  |
| Low | Medium | High |
| Low | Non – actual | Non – actual | Actual |
| Medium | Non – actual | Actual | Actual |
| High | Actual | Actual | Actual |
| Very high | Actual | Actual | Actual |

**Consequences of a data security breach**

**Possible consequences of the implementation of threats of various classes**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| N | Type of attack | | Possible consequences |
| 1 | Network traffic evaluation | | The study of network traffic features and the interception of transmitted information, such as user identification and passwords. |
| 2 | Network "Password" surveillance assault | | This text pertains to various aspects of network communication and security, including the definition of protocols, the identification of available ports for network services, the laws governing the formation of connection identifiers, the identification of active network services, and the use of user IDs and passwords for authentication purposes. |
| 3 | Replacement of a reliable network object | | Engaging in any form of malicious activity aimed at gaining unauthorized access. |
| 4 | Imposing a fictitious itinerary | | The act of altering the path of messages, unauthorized modification of routing, and address information. The act of gaining entry to network resources without proper authorization and the dissemination of fabricated information. |
| 5 | Inclusion of a bogus network object | | The act of altering route and address data without proper authorization, manipulating transmitted data, and disseminating false messages. |
| 6 | Network traffic evaluation | | The act of intercepting and observing network traffic. The act of gaining entry to network resources without proper authorization and the dissemination of fabricated information. |
| 7 | Denial of service | The phenomenon of partial depletion of resources. | The diminution of communication channel bandwidth has an impact on the efficacy of network equipment. The diminished functionality of server applications. |
|  |  | The complete depletion of resources. | The incapacity to convey messages owing to inadequate access to the transmission medium and the inability to establish a connection. The act of declining to offer a particular service, such as electronic mail or file sharing. |
|  |  | The breach of logical coherence among attributes, data, and objects. | The failure to convey messages owing to the absence of accurate routing and addressing information. The unauthorized modification of identifiers, passwords, and other related information may result in the inability to receive services. |
|  |  | Leveraging program errors for specific purposes. | The impairment of network device functionality. |
| 8 |  | By sending files containing destructive executable code, virus infection | The compromise of confidentiality, integrity, and availability of information. |
|  | Remote application launch | Through the act of overflowing the buffer of the server application, it is possible to exploit vulnerabilities in the system. |  |
|  |  | Through the utilization of remote system management functionalities offered by concealed software and hardware bookmarks or conventional tools. | The concept of managing systems in a covert manner. |

In most cases, there are four stages involved in the process of putting the threat into action. These stages are information gathering, intrusions (also known as infiltrations into the working environment), unlawful access, and the eradication of signs of unauthorized access.

During the phase of collecting information, the violator may be interested in a variety of facts regarding the ISPD, such as the following: a) information regarding the topology of the network in which the system runs. At the same time, one can conduct an investigation into the neighborhood surrounding the network (for instance, the intruder may be interested in the addresses of trustworthy hosts that are less safe). For example, the ping command can be used to send ECHO\_REQUEST ICMP queries with the anticipation of receiving ECHO\_REPLY ICMP responses to them. This allows one to determine whether or not a host is available to receive those requests. There are utilities such as fping that perform parallel assessment of the availability of hosts. These utilities are able to scan a significant portion of the address space in a very short amount of time to determine whether or not hosts are available in that region. The "node counter" (also known as the distance between hosts) is frequently used as the basis for determining the topology of the network. In this scenario, techniques like "TTL modulation" and route recording may be utilized as potential solutions. Modulating the TTL field of IP packets is the "TTL modulation" approach, which is implemented by the traceroute software (for Windows NT, tracert.exe). This method may be found in the documentation for the traceroute program. The route can be recorded using the ICMP packets that are created when you run the ping command.

The collection of information can also be based on requests. These requests can be made as follows: to the DNS server for the list of registered (and probably active) hosts; to a router based on the RIP protocol for information regarding known routes (network topology information); incorrectly configured devices that support the SNMP protocol (network topology information). It is possible to collect information about the configuration of the firewall (ME) and the topology of the ISPD behind the ME, including by sending packets to all ports of all the intended hosts of the internal (protected) network; b) about the type of operating system (OS) in the ISPD, if the ISPD is located behind the firewall (ME). The most well-known method for determining the type of host operating system is based on the fact that different OS types implement the requirements of the RFC standards for the TCP/IP stack in a different manner. This is the case because different OS types implement the TCP/IP stack differently. The intruder will be able to remotely determine the sort of operating system that is installed on the ISPD server by sending specially created requests and examining the responses they receive to those requests.

There are specialized applications available, like as Nmap and QueSO, that can put these strategies into action. It is also feasible to notice that such a way of detecting the OS type is the simplest request to create a connection using the telnet remote access protocol (telnet connection). As a consequence of this request, the "appearance" of the response can be used to determine the kind of host operating system. The presence of particular services can also be used as an extra feature to detect the type of operating system (OS) used by the host; c) information regarding the services that are currently being used by the hosts. The method of identifying "open ports" is the foundation for the definition of services that are carried out on the host. The purpose of this method is to gather information about the availability of the host. For instance, in order to determine whether or not a UDP port is available, it is necessary to receive a response after sending a UDP packet to the port in question. If an ICMP PORT UNREACHEBLE message is received in response, this indicates that the service in question is not available; on the other hand, if this message is not received, this indicates that the port in question is "open."

The protocol that is utilized in the TCP/IP protocol stack has a significant impact on the application of this technology, which can result in a wide variety of possible outcomes. There have been a lot of different software programs developed to help automate the process of collecting information about ISPD. The following can serve as an illustration of this point:

1) Strobe and Portscanner are optimal methods for detecting accessible services based on TCP port polling; 2) Nmap is a program for scanning available services that was created for Linux, FreeBSD, Open BSD, Solaris, and Windows NT; Strobe and Portscanner are both available online. At the moment, it is the most common method of scanning network services;

3) Queso is a high-precision tool for finding the operating system (OS) of a network host by delivering a sequence of correct and wrong TCP packets, examining the response, and comparing it with a variety of known replies from various operating systems. This method is used to determine the OS of a network host. This tool is also widely used as a scanning tool in modern times;

4) The Cheops network topology scanner gives you the ability to obtain the network topology, providing you with a picture of the domain, IP address areas, and other relevant information. In this particular instance, the host operating system and any potential network devices (printers, routers, etc.) are identified;

5) Firewalk is a scanner that builds a network topology and determines the configuration of a firewall by employing the techniques of the traceroute program. This is done in order to analyze the response to IP packets and determine the configuration of the firewall.

During the intrusion stage, it is studied whether or not usual vulnerabilities exist in the system services or whether or not errors occurred during system administration. When vulnerabilities are exploited successfully, the offending process typically obtains a privileged execution mode (access to the privileged execution mode of the command processor), enters an unauthorized user account into the system, obtains a password file, or disrupts the operability of the attacked host. Other possible outcomes include gaining access to the privileged execution mode of the command processor.

This stage of the development of a threat typically consists of multiple phases. The phases of the process of implementing a threat may include, for instance: establishing communication with the host against which the threat is being implemented; vulnerability detection; the introduction of a malicious program in the interests of expanding rights; and other similar activities.

Threats that are implemented during the intrusion stage are separated into several categories according to the levels of the TCP/IP protocol stack. This is because threats can be produced at either the network, transport, or application level, depending on the type of intrusion mechanism that is being utilized. The following are examples of risks that are often implemented at the network and transport levels: a threat aimed at replacing a trusted object; b) a threat aimed at creating a false route in the network; c) threats aimed at creating a false object using the shortcomings of remote search algorithms; d) denial of service threats based on IP defragmentation, on the formation of incorrect ICMP requests (for example, the "Ping of Death" and "Smurf attack"), on the formation of incorrect TCP requests (the "Land attack"), on the

Threats that target the unauthorized launch of applications, threats whose implementation is associated with the introduction of program bookmarks (such as a "Trojan horse"), threats that target the identification of passwords for access to the network or to a specific host, etc. are examples of typical threats that are implemented at the application level. If the implementation of the threat does not result in the violation receiving the highest access rights within the system, then attempts may be made to extend these rights to the highest level that is possible. In order to accomplish this goal, it is possible to utilize vulnerabilities not just for network services but also vulnerabilities in the system software of ISPD hosts. The actual accomplishment of the purpose of implementing the threat is carried out at the level of the implementation of illegal access: A breach of confidentiality occurs when there is unauthorized copying or distribution, a breach of integrity occurs when there is destruction or modification, and a breach of accessibility occurs when there is blocking.

At the same time, following these acts, there is typically the formation of what is known as a "black entrance." This "black entrance" takes the form of one of the services (daemons) that serves a particular port and carries out the directives of the violation. The "back entrance" is left in the system in order to ensure the following: the ability to gain access to the host even if the administrator eliminates the vulnerability that was used for the successful implementation of the threat; opportunities to access the host in as stealthily a manner as is possible; the ability to access the host quickly (without having to repeat the process of implementing the threat again); and the ability to access the host without having to repeat the process of implementing the threat.

The intruder has the ability to introduce a malicious program into the network or to a specific host by using the "black entrance." One example of such a program is a password sniffer, which is designed to extract user ids and passwords from network traffic when high-level protocols (such as ftp, telnet, or rlogin) are functioning. Malware can be implemented to target authentication programs and identification, network services, the operating system kernel, the file system, libraries, and other components of the system, among other things.

In the final step of the process, which is called "eliminating traces of the threat," an effort is made to eradicate any remnants of the violator's behavior. At the same time, the relevant records are removed from any and all audit logs that could possibly contain them, and this includes records that document the information gathering itself.

**Conclusion**

The purpose of this diploma research was to investigate the security threat model of information held by credit organizations. The findings of this investigation were intended to provide significant insights and recommendations for improving the information security held by credit businesses. This research has gained a complete understanding of the security threats that credit organizations face and evaluated the efficiency of current security measures by using a mixed-methods strategy that combines interviews and thematic analysis. This technique has enabled the researchers to use a mixed-methods approach. This research has gained extensive insights into the experiences, perspectives, and issues that key stakeholders face in relation to security threats through the use of qualitative interviews with those stakeholders. These key stakeholders include IT security professionals, managers, and employees. The data from the interviews were analyzed using a thematic approach, which led to the discovery of repeating themes, patterns, and linkages. This helped shed light on the complex nature of security threats faced by credit organizations. The investigation has produced a comprehensive understanding of both the internal and the external dangers, such as dishonest behavior on the part of employees, insider attacks, hacking, and phishing, as well as emerging threats like ransomware and AI-powered attacks. In addition to that, our study has conducted an in-depth analysis and evaluation of the current security measures that are in place at credit institutions. This study has found potential holes and weaknesses in the security architecture by determining how effective the present countermeasures are. These findings contribute to the ongoing efforts to strengthen the security posture of credit companies, ensuring the protection of sensitive customer information and limiting potential risks. [Credit firms are] tasked with ensuring the protection of sensitive customer information and mitigating potential hazards. Even though this study did not make use of surveys, the qualitative technique and thematic analysis were able to provide extremely helpful insights into the security threat model of information pertaining to credit organizations. The absence of surveys does not lessen the value of the findings because the interviews have collected in-depth viewpoints and experiences of key players, revealing nuanced understandings of the security landscape. Moreover, the findings have been validated by the fact that the interviews have been conducted.

This research offers practical recommendations to credit organizations for enhancing their security threat model, and it does so on the basis of the findings of the research. These proposals can involve making technical advancements, revising company policies, organizing employee training programs, or working together with industry experts and regulatory organizations. Credit institutions have the ability to improve their existing security architecture and build proactive measures to successfully prevent possible risks if they put these ideas into action and implement them. It is essential to recognize the constraints that were placed on this study. The absence of surveys resulted in a smaller than usual sample size, which may have an impact on the extent to which the findings can be generalized. In addition, the research was carried out within a particular timeframe, which may have limited the amount of depth and breadth of the data that was gathered. In spite of this, the insights that were gathered from this research contribute to a better knowledge of the security threat model of information held by credit organizations, as well as providing a framework for additional research in this subject.

In summary, the findings of this diploma research have shed light on the security challenges that credit businesses face and evaluated the effectiveness of the various security solutions that are currently in place. It has done so by conducting qualitative research and theme analysis, and as a result, it has provided credit organizations with useful insights as well as recommendations for improving their security posture. Credit institutions can protect their precious information assets, maintain their customers' trust, and secure the integrity and stability of the financial ecosystem if they take preventative measures to address the dangers described above.