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»

Astana, 2023

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

**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.

**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.

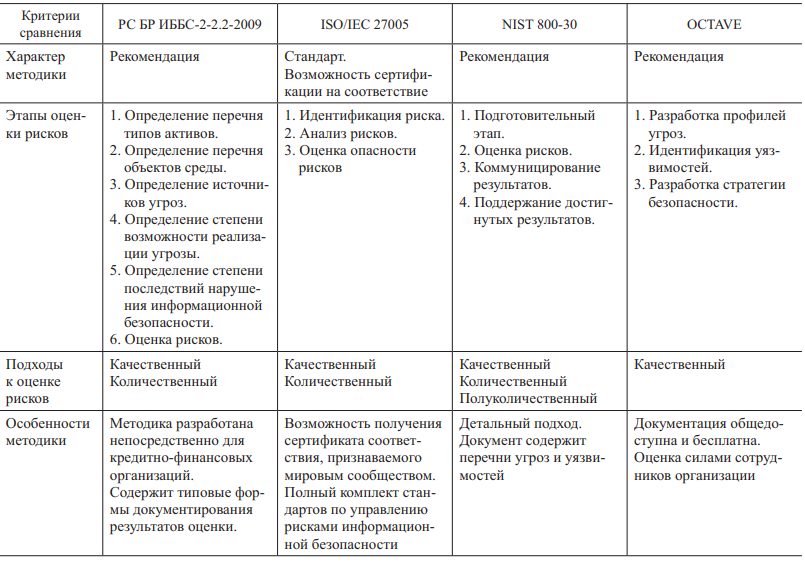
To determine the level of initial security (aka the initial security coefficient Y1), you need to select one of the values that is most suitable for your system for seven indicators.

List of characteristics and their values:

|  |  |  |  |
| --- | --- | --- | --- |
| technical and operational characteristics of ispdn | security level | | |
| high | medium | low |
| 1. by territorial placement: | | | |
| distributed ispdn, which covers several regions, territories, districts or the state as a whole | - | - | + |
| urban ispdn, covering no more than one locality (city, village) | - | - | + |
| corporate distributed ispdn, covering many divisions of one organization | - | + | - |
| local (campus) ispdn, deployed within one building | - | + | - |
| local ispdn, deployed within one building | + | - | - |
| 2. by the presence of a connection to public communication networks: | | | |
| ispdn having multipoint access to the public communication network ispdn having single-point | - | - | + |
| access to the public communication | - | + | - |
| network ispdn 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: | | | |
| ispdn, to which the employees of the organization that is the owner of ispdn have access, or the subject | - | + | - |
| of the ispdn pd, to which all employees of the organization that is the owner of ispdn have access | - | - | + |
| with open access | - | - | + |
| 5. by the presence of connections with other pd databases of other ispdn: | | | |
| an integrated ispdn (organization) uses several ispdn pd databases, while the organization is not the owner of all the pd databases used) | - | - | + |
| ispdn, which uses one pd database belonging to the organization that owns this ispdn | + | - | - |
| 6. by the level of generalization (depersonalization) of pd: | | | |
| ispdn, in which the data provided to the user is depersonalized (at the level of the organization, industry, region, region, etc.) | + | - | - |
| ispdn, in which the data is depersonalized only when transferred to other organizations and is not depersonalized when provided to the user in | - | + | - |
| the ispdn 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 ispdn users without pre-processing | | | |
| ispdn, providing the entire database with | - | - | + |
| ispdn pd, providing part | - | + | - |
| of ispdn 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:

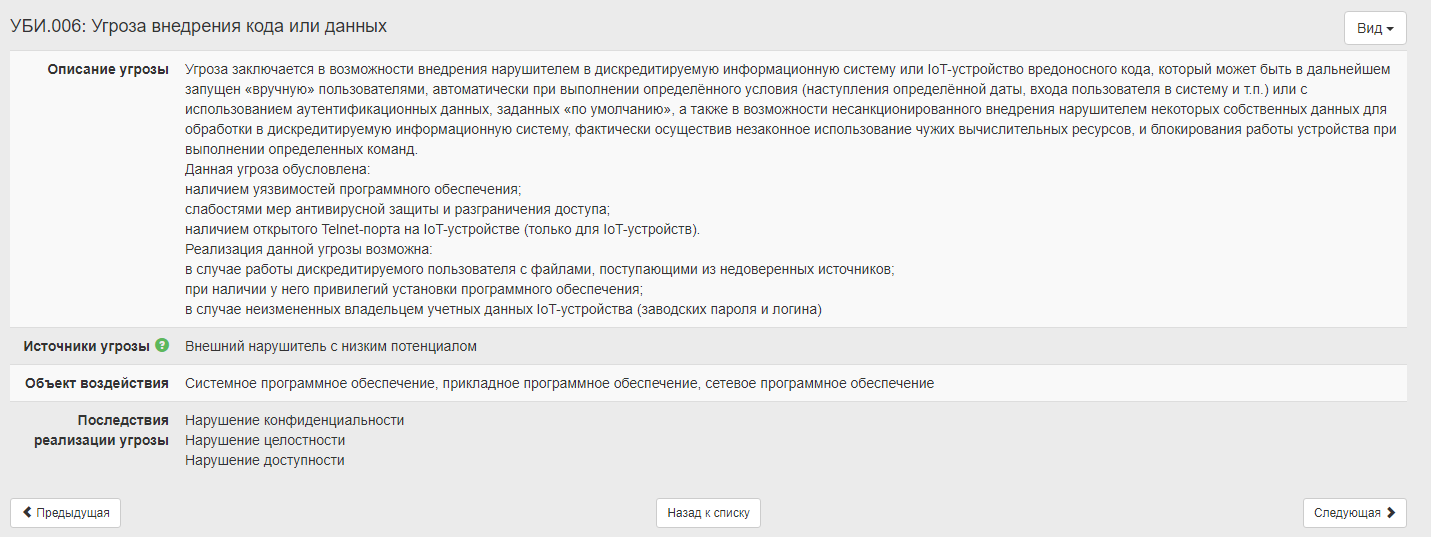
exclusion of threats associated with grid systems, supercomputers, and large amounts of data; exclusion of threats associated with virtualization; exclusion of threats associated with the use of wireless communication networks; exclusion of threats associated with the use of cloud services; exclusion 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 ISPDn 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 ISPDn, 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 ISPDn 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 ISPDn, if the ISPDn 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 ISPDn 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 ISPDn. 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 ISPdn 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.