МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій

Кафедра авіаційних комп’ютерно-інтегрованих комплексів

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач випускової кафедри

_______Віктор СИНЄГЛАЗОВ

“_____”_____________2023 р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ

“БАКАЛАВР”

Спеціальність 151 “Автоматизація та комп'ютерно-інтегровані технології ”

Освітньо-професійна програма “Комп'ютерно-інтегровані технологічні процеси і виробництва”

Тема: “ Система технічного захисту комп’ютерних мереж підприємств цивільної авіації ”

Виконавець: студент групи КП-404Ба Костянтин ДЖЕЛАЛОВ

Керівник: кандидат технічних наук, доцент Олег СМІРНОВ

Нормоконтролер: ____________Микола ФІЛЯШКІН

Київ - 2023

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

NATIONAL AVIATION UNIVERSITY

Faculty of Aeronautics, Electronics and Telecommunications

Department of aviation computer-integrated complexes

ADMIT TO DEFENSE

Head of the graduation department

______Viktor SINEGLAZOV

"____"____________2023

QUALIFICATION WORK

(EXPLANATORY NOTE)

GRADUATE DEGREE OF EDUCATION

"BACHELOR"

Specialty 151 "Automation and computer-integrated technologies"

Educational and professional program "Computer-integrated technological processes and production"

Topic: " Computer network technical protection system in civil aviation enterprises "

Executor:	student of group KP-404Ba Kostiantyn DZHELALOV
Supervisor:	PhD, professor assistant Oleg SMIRNOV
Normocontroller:	_____Mykola FILIASHKIN

Kyiv – 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій

Кафедра авіаційних комп'ютерно-інтегрованих комплексів

Освітній ступінь: бакалавр

Спеціальність 151 «Автоматизація та комп'ютерно-інтегровані технології»

Освітньо-професійна програма «Комп'ютерно-інтегровані технологічні процеси і виробництва»

ЗАТВЕРДЖУЮ

Завідувач кафедри

______Віктор СИНЄГЛАЗОВ

"_____"____________2023 р.

ЗАВДАННЯ

на виконання кваліфікаційної роботи студента

Джелалова Костянтина Олександровича

1. **Тема роботи:** " Система технічного захисту комп'ютерних мереж підприємств цивільної авіації ".
2. **Термін виконання роботи:** з 23.05.2023р. по 20.06.2023р.
3. **Вихідні дані до роботи:** Розробка системи технічного захисту комп'ютерних мереж підприємств цивільної авіації. Забезпечення безпеки і конфіденційності даних, що обробляються в комп'ютерних мережах підприємств цивільної авіації.
4. **Зміст пояснювальної записки (перелік питань, що підлягають розробці):** Аналіз і оцінка потенційних загроз безпеці комп'ютерних мереж підприємств цивільної авіації. Розробка стратегії технічного захисту комп'ютерних мереж з урахуванням специфіки галузі цивільної авіації.
5. **Перелік обов'язкового графічного матеріалу:** Структурна схема підмережі корпоративної комп'ютерної мережі. Загальна структура системи захисту інформації в локальній мережі аеропорту. Внутрішня структура доменів безпеки.

6. Календарний план-графік

Етапи виконання дипломного проекту (роботи)	Термін виконання роботи	Примітка
1.1. Актуальність та значущість теми для практичної діяльності	23.05 – 24.05	Виконано
1.2. Мета та завдання дослідження	24.05 – 25.05	Виконано
1.3. Опис об'єкта дослідження та його характеристика	25.05 – 26.05	Виконано
2.1. Основні поняття та визначення, що стосуються технічного захисту комп’ютерних мереж	28.05 – 29.05	Виконано
2.2. Методи захисту комп'ютерних мереж	29.05 – 30.05	Виконано
2.3. Системи технічного захисту комп'ютерних мереж	30.05 – 02.06	Виконано
2.4. Специфіка технічного захисту комп'ютерних мереж цивільної авіації	02.06 – 04.06	Виконано
3.1. Аналіз існуючої системи технічного захисту комп'ютерних мереж цивільної авіації	04.06 – 05.06	Виконано
3.2. Розробка та пропозиція вдосконалень системи технічного захисту комп'ютерних мереж цивільної авіації	05.06 – 12.06	Виконано
3.2.1. Симуляційне середовище	05.06 – 06.06	Виконано
3.2.2. Топологія мережі	06.06 – 07.06	Виконано
3.2.3. Організація вузлів мережі	07.06 – 08.06	Виконано
3.3. Перевірка та оцінка ефективності розроблених удосконалень	11.06 – 12.06	Виконано
4.1. Основні результати дослідження	13.06 – 14.06	Виконано
4.3. Перспективи подальших досліджень теми	16.06 – 17.06	Виконано
5.1. Огляд літератури за темою дослідження	18.06 – 19.06	Виконано
5.2. Список використаних джерел	19.06 – 20.06	Виконано

7. Дата видачі завдання ____

Керівник: _____Олег СМІРНОВ

Завдання прийняв до виконання ______Костянтин ДЖЕЛАЛОВ

NATIONAL AVIATION UNIVERSITY

Faculty of Aeronautics, Electronics and Telecommunications

Department of aviation computer-integrated complexes

Educational degree: Bachelor

Specialty 151 "Automation and computer-integrated technologies"

Educational and professional program "Computer-integrated technological processes and production"

APPROVED
Head of Department
_______Viktor SINEGLAZOV
"____"___________2023

TASK

For the student's qualification work

Dzhelalov Kostiantyn Olexandrovich

1. The thesis title: " Computer network technical protection system in civil aviation enterprises ".

2. The term of the project: from 23.05.2023 until 20.06.2023

3. Output data to the project: Development of a system of technical protection of computer networks of civil aviation enterprises. Ensuring security and confidentiality of data processed in computer networks of civil aviation enterprises.

4. Contents of the explanatory note: Analysis and assessment of potential threats to the security of computer networks of civil aviation enterprises. Development of a strategy for technical protection of computer networks taking into account the specifics of the civil aviation industry.

5. List of required illustrative material: Structure diagram of a corporate computer network subnet. The general structure of the information protection system in the airport's local network. Internal structure of security domains.

6. Planned schedule.

Task	Execution term	Execution mark
1.1. Relevance and significance of the topic for practical activities	23.05 – 24.05	Performed
1.2. Aim and objectives of the research	24.05 – 25.05	Performed
1.3. Description of the research object and its characteristics	25.05 – 26.05	Performed
2.1. Key concepts and definitions related to technical protection of computer networks	28.05 – 29.05	Performed
2.2. Methods of protecting computer networks	29.05 – 30.05	Performed
2.3. Technical protection systems for computer networks	30.05 – 02.06	Performed
2.4. Specifics of technical protection of computer networks in civil aviation	02.06 – 04.06	Performed
3.1. Analysis of the existing technical protection system for computer networks in civil aviation	04.06 – 05.06	Performed
3.2. Development and proposal of improvements for the technical protection system for computer networks in civil aviation	05.06 – 12.06	Performed
3.2.1. Simulation environment	05.06 – 06.06	Performed
3.2.2. Network topology	06.06 – 07.06	Performed
3.2.3. Network nodes organization	07.06 – 08.06	Performed
3.3. Testing and evaluation of the effectiveness of the developed improvements	11.06 – 12.06	Performed
4.1. Main research results	13.06 – 14.06	Performed
4.3. Perspectives for further research on the topic	16.06 – 17.06	Performed
5.1. Literature review on the research topic	18.06 – 19.06	Performed
5.2. List of used sources	19.06 – 20.06	Performed

7. Issue date of the task____

Supervisor: _____Oleg SMIRNOV

The task was accepted by: ______Kostiantyn DZHELALOV

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи :«Система технічного захисту комп'ютерних мереж підприємств цивільної авіації»

КОМП’ЮТЕРНА МЕРЕЖА, СИСТЕМА ТЕХНІЧНОГО ЗАХИСТУ ЛОКАЛЬНОЇ МЕРЕЖІ, ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ МЕРЕЖІ НА ПІДПРИЄМСТВАХ ЦИВІЛЬНОЇ АВІАЦІЇ

Предмет дослідження – Система технічного захисту комп'ютерних мереж підприємств цивільної авіації.

Мета кваліфікаційної роботи – розробка та ефективна імплементація системи технічного захисту комп'ютерних мереж в галузі цивільної авіації

Метод дослідження – аналіз літературних джерел, порівняльний аналіз різних методів технічного захисту, практичне впровадження системи технічного захисту.

Об'єкт дослідження – комп'ютерні мережі підприємств цивільної авіації.

Результати дослідження показали, що використання комплексної системи технічного захисту, включаючи файерволи, системи контролю доступу та антивірусні програми, ефективно забезпечує безпеку комп'ютерних мереж у галузі цивільної авіації.

Розроблено стратегію технічного захисту, яка враховує специфіку галузі цивільної авіації та вимоги регуляторних органів. Впровадження системи технічного захисту на підприємствах цивільної авіації дозволяє підвищити рівень безпеки мереж та контролювати доступ до конфіденційної інформації.

Результати кваліфікаційної роботи рекомендуються для використання в практичній діяльності підприємств цивільної авіації для забезпечення безпеки їх комп'ютерних мереж. Розроблені рекомендації та методи можуть бути використані як основа для подальших досліджень у галузі

ABSTRACT

Explanatory note of the qualification work: "System of technical protection of computer networks of civil aviation enterprises"

COMPUTER NETWORK, LOCAL NETWORK TECHNICAL PROTECTION SYSTEM, RESEARCH OF NETWORK PROTECTION METHODS AT CIVIL AVIATION ENTERPRISES

The subject of the study is the system of technical protection of computer networks of civil aviation enterprises.

The purpose of the qualification work is the development and effective implementation of a system of technical protection of computer networks in the field of civil aviation

Research method – analysis of literary sources, comparative analysis of various technical protection methods, practical implementation of the technical protection system.

The object of research is computer networks of civil aviation enterprises.

The results of the study showed that the use of a complex system of technical protection, including firewalls, access control systems and anti-virus programs, effectively ensures the security of computer networks in the field of civil aviation.

A technical protection strategy has been developed, which takes into account the specifics of the civil aviation industry and the requirements of regulatory authorities. Implementation of the technical protection system at civil aviation enterprises allows to increase the level of network security and control access to confidential information.

The results of the qualification work are recommended for use in the practical activities of civil aviation enterprises to ensure the security of their computer networks. The developed recommendations and methods can be used as a basis for further research in the field

CONTENT

INTRODUCTION

Today's world is defined by the rapid development of technologies that change the way we live, work and interact. In this modern digital landscape, computer networks are becoming a major component of our connected world, enabling the transmission, processing and exchange of vast amounts of information.

However, along with the growing importance of computer networks, there are new threats related to misuse, unauthorized access and cyber-attacks. These threats can lead to serious consequences, such as leakage of confidential data, violations of security and functioning of systems, as well as financial losses.

In this context, the relevance of the topic of protecting computer networks becomes obvious. The development of effective technical solutions and protection strategies is becoming a necessity to ensure the security and stability of computer networks in all spheres of activity, including business, government agencies and critical infrastructure.

The purpose of this work is research and development of technical solutions aimed at protecting computer networks from various threats. This includes analysis of modern protection methods and protocols, detection of vulnerabilities, development of preventive measures, improvement of incident detection and response mechanisms.

To achieve the goal, the work involves the use of various research methods, such as a literature review, experimental tests, analytical models, and mathematical modeling. These methods will allow a deeper understanding of the essence of the problem and the development of effective and innovative solutions.

The obtained research results have not only theoretical significance, but also great practical application. The developed technical solutions and recommendations can be used in real computer networks to ensure their security and reliability.

CHAPTER 1
INTRODUCTION

1.1. Relevance and significance of the topic for practical activities

In the current digital era, where information security is essential for the efficient operation of businesses and organizations, the topic of " Computer network technical protection system in civil aviation enterprises" is quite pertinent. Businesses in the civil aviation industry deal with sensitive information that must be safeguarded from cyberattacks and illegal access, such as passenger information, flight itineraries, and other private data.

A compromise in the security of a civil aviation company's computer networks can have serious financial repercussions, legal repercussions, and reputational damage. Therefore, in order to protect against cyber threats, a strong technical protection system must be in place.

The fact that this topic offers rules and advice for creating an efficient technological protection system for computer networks in civil aviation firms makes it significant for practical activities. Organizations will benefit from its assistance in developing strategies for risk mitigation, identifying and evaluating potential risks and vulnerabilities, and improving the security posture of their computer networks.

The critical nature of the aviation industry further emphasizes the topic's importance. Any disruption to the computer networks could have detrimental effects because the safety and security of the passengers, crew, and aircraft are of the utmost importance.

In order to organize and regulate flights, track weather, and communicate with ground staff, the aviation sector also significantly relies on computer networks. Any disruption or malfunction of these systems may cause cancellations, delays, and even unsafe circumstances.

Therefore, it is essential for maintaining the safe and successful functioning of the sector that an appropriate technical protection system for computer networks in civil aviation firms is developed and put in place. It necessitates having a thorough awareness of the unique requirements and problems faced by the aviation industry, as well as the capacity to implement cutting-edge cybersecurity solutions to reduce risks and safeguard important resources.

Overall, because it offers insights into best practices and techniques for increasing information security and defending against cyber threats, this topic is significant and pertinent for practical actions in the aviation industry.

Additionally, a multi-layered strategy is needed for the development of technological protection solutions for computer networks in civil aviation firms. This entails implementing a range of security measures, including as access control guidelines, firewalls, intrusion detection systems, anti-malware software, and encryption methods. Additionally, it calls for developing incident response strategies to deal with potential security breaches and educating staff members on cybersecurity best practices.

Additionally, to find any vulnerabilities in their computer networks and execute fixes, civil aviation businesses should perform routine security audits and assessments. Additionally, they should keep abreast of the most recent trends and advancements in cybersecurity so that they may modify their security measures as necessary.

It is important to remember that putting in place a technical protection system is a continuous process that calls for ongoing upgrades and enhancements. The cybercriminal threat landscape is continually changing, and attacks are getting more advanced. In order to guard against potential security breaches, civil aviation businesses must be diligent and aggressive in securing their computer networks.

In the current electronic age, the subject of " Computer network technical protection system in civil aviation enterprises" is of utmost significance. The requirement for a strong technical protection system to guard against cyber threats is underscored by the aviation industry's crucial nature and the sensitive information it handles. Civil aviation businesses should have a multi-layered strategy for cybersecurity, which includes using a variety of security measures, conducting regular security audits and assessments, and training staff on best practices. Civil aviation businesses can lower the risk of security lapses and guarantee the safe and effective running of their operations by putting in place an efficient technical protection system.

1.2. Aim and objectives of the research

The research's objective is to create an efficient technical protection solution for computer networks in civil aviation businesses that will strengthen information security and safeguard against online threats.

The following goals have been selected in order to fulfill this intention:

To review the research on technical network protection systems and cybersecurity in the civil aviation industry: This objective entails completing a thorough analysis of the body of knowledge about technical network protection systems and cybersecurity in the civil aviation sector. The review will incorporate academic and business-related research publications, reports, case studies, and best practices.

To ascertain the specific challenges and requirements of the aviation industry in developing and implementing a technical protection system for computer networks: In order to develop and put into place a technical defensive system for their computer networks, this goal seeks to identify the special difficulties and demands of the civil aviation sector. This could, for instance, entail looking into the precise laws and guidelines governing aviation cybersecurity or the specific categories of data that require protection.

To assess the current system of technical protection for computer networks in civil aviation companies and identify areas for improvement: To do this, it is necessary to evaluate the existing system of technical protection for computer networks in civil aviation companies and pinpoint opportunities for improvement. This could entail examining prospective threats that the current system might not be able to manage, assessing the efficacy of current security measures, or detecting vulnerabilities.

To develop and propose enhancements to the current system of technical protection for computer networks in commercial civil aviation: This objective entails creating and proposing specific changes to the technological protection system for computer networks in civil aviation firms based on an evaluation of the current system. These can involve putting in place fresh security measures, modernizing current processes, or incorporating new technologies.

To test and evaluate the anticipated improvements to the technical protection system: Last but not least, this objective entails putting the suggested technological protection system modifications to the test and evaluating how well they work to improve information security and protect against online threats. This could entail testing the system's defenses against simulated cyberattacks or compiling information on security occurrences both before and after the enhancements were put in place. The evaluation's findings will be used to further hone and enhance the technical protection system.

Overall, the research intends to offer advice and instructions for civil aviation firms to create and put into place an efficient system of technological protection for their computer networks, to improve information security, and to safeguard against cyber attacks.

By shedding light on the particular difficulties and needs of this business, the research will advance the subject of aviation cybersecurity. A technical protection system for computer networks will also be developed and put into place using the best practices and methods identified.

There will be theoretical and applied components to the research. The theoretical portion will entail reading up on technical defense mechanisms, cybersecurity, and issues unique to the aviation sector. The practical portion will entail reviewing the current technical protection system, creating and suggesting improvements, testing the proposed improvements, and assessing their efficacy.

The aviation industry is becoming more and more dependent on computer networks and information systems, hence research on the "System of technical protection of computer networks of civil aviation enterprises" is crucial. This reliance generates new points of vulnerability and openings for cyberattacks, which might have detrimental effects on aviation security and safety.

Information security is governed by stringent rules and standards in the aviation business as well, and failing to adhere to these rules can have major repercussions, such as penalties, legal liability, and reputational harm.

The research intends to assist firms in complying with these requirements, lowering their vulnerability to cyber threats, and enhancing their overall information security posture by building an efficient system of technical protection for computer networks in civil aviation enterprises.

By identifying best practices and tactics for safeguarding vital infrastructure, such as computer networks in the aviation industry, the research will also contribute to the larger subject of cybersecurity. Other companies and sectors can improve their cybersecurity posture by using this knowledge.

Overall, the study on the " Computer network technical protection system in civil aviation enterprises" has important applications and can advance cybersecurity research as well as the safety and security of the aviation sector.

1.3. Description of the research object and its characteristics

The technological network protection system used by businesses involved in civil aviation is the study's research subject.

Organizations engaged in air transport activities, such as airlines, airports, air traffic control organizations, and other associated companies, are referred to as civil aviation enterprises. The daily operations of these companies, including flight planning, scheduling, passenger handling, cargo management, and air traffic control, significantly rely on computer networks and information systems.

The set of methods, tools, and procedures used to defend these networks and systems against online dangers is referred to as the technical protection system for computer networks in civil aviation firms. Firewalls, intrusion detection and prevention systems, antivirus and antimalware software, encryption, access controls, and other security measures are some of the protection systems that are used.

The following are aspects of the computer network technical protection system used by civil aviation businesses:

Criticality: To ensure safe and secure operations, the protection system utilized by civil aviation firms is essential. Any system flaw or security breach can lead to serious operational disruptions, safety dangers, and monetary losses. For instance, a cyber attack on a flight management system may jeopardize the security of the crew and passengers, with disastrous results. Therefore, the defense system needs to be built to effectively foresee, identify, and react to future threats and attacks. To protect against cyber attacks, this entails putting in place firewalls, intrusion detection systems, and other security measures.

Complexity: With many interrelated parts, the computer networks and information systems employed in the civil aviation industry are complicated. The security measures must be dependable and effective while the protection system can manage this complexity. This entails making sure the system is adaptable, scalable, and able to respond to emerging technologies and shifting operational needs.

An ever-evolving threat environment: New dangers and attack vectors are regularly appearing in the threat environment for civil aviation firms. In order to properly counter these new threats, the defense system must be dynamic and adaptable. To ensure that the system can survive the most recent cyber attacks, this means periodically updating it with the newest security patches and upgrades.

Requirements for compliance: In order to ensure secure operations, civil aviation enterprises must abide by a number of safety and cybersecurity rules, including ICAO Annex 17 and the FAA CSMS framework. To be in compliance with these regulations, the protective system must meet particular standards and requirements. To comply with these rules, this entails putting in place security controls like access control, data encryption, and incident response processes.

Integration with other systems: To maintain smooth and secure operations, the protective system utilized for computer networks in the civil aviation industry must integrate with other operational and safety-critical systems. Integration is necessary to make it easier for people to share data and information, which is crucial for company operations. It is crucial to make sure that the security system can recognize and stop unwanted access to critical data because this integration might potentially bring up new security threats.

Human variables: The awareness, training, and behavior of the employees can significantly affect the effectiveness of the safety system. For instance, it is vital to make sure that staff are properly taught and informed of the potential hazards because they may unwittingly fall prey to social engineering attacks. Employees may unwittingly cause security flaws by using weak passwords or neglecting to apply security updates, for example. In order to ensure that personnel are aware of security concerns and are able to recognize possible threats, the protective system must incorporate measures to that effect.

Cost considerations: A protective system's installation and upkeep demand substantial financial and human resources. In order to provide dependable and efficient security measures, it is crucial to allot enough resources to ensure that the protective system is properly planned, put into place, and maintained. This involves investing in the most recent security technologies to make sure the system can withstand the most recent cyber threats and hiring cybersecurity specialists to oversee the system.

1.4. Research methods

To achieve its stated objectives, the research will employ the following methods:

A detailed analysis of the body of existing literature will be done in order to ascertain the current level of knowledge on the technical protection of computer networks in civil aviation companies. Examining published publications, research papers, reports, and other pertinent materials pertaining to technical protection systems in civil aviation will be part of the literature review.

Case Study: Using a case study methodology, the technical protection system of a specific civil aviation company will be studied. The case study method will give a thorough understanding of the technological security system in use and aid in identifying areas that need strengthening. The defense system's effectiveness, efficiency, and vulnerabilities will need to be thoroughly investigated.

Interviews: Interviews with experts in the sectors of civil aviation and computer network defense will be conducted in order to gain insight into current practices, challenges, and development areas. The interviews will offer qualitative data and aid in identifying the problems experts encountered when putting the protective mechanism in place.

Testing: To ascertain the effectiveness of suggested protective system modifications, experiments and testing will be conducted under simulated or real-world conditions. This strategy will offer numerical information that may be used to gauge the success of the suggested improvements.

Combining these methods will provide a comprehensive and all-inclusive method for assessing the technological protection system of computer networks in civil aviation companies and identifying potential development areas. This research strategy will make it possible to fully comprehend the technical protection system, which is necessary for creating a protective system that works.

The literature research and case study approaches will give you a thorough understanding of how computer networks in civil aviation companies are protected technologically. The evaluation of the literature will make it possible to pinpoint important problems, obstacles, and knowledge gaps in the field. The case study method will assist in determining the technical security system's advantages, disadvantages, and potential development areas.

The effectiveness of the suggested protection system upgrades will be evaluated using the trial and testing methodology. To do this, the proposed modifications will be tested in simulated or real-world scenarios, and their effectiveness will be contrasted with that of the current protective system. This will make it easier to assess the effectiveness of the suggested modifications and their potential effects on the defense system.

Overall, the combination of these methods will provide a robust and comprehensive strategy for examining the technological security of computer networks in civil aviation companies and formulating effective plans for boosting the efficacy and efficiency of the defense system. The study will offer suggestions for enhancing the current security system and creating fresh, efficient security measures.

Additionally, data analytic techniques will be used to analyse and evaluate the collected data. Depending on the type of data, both quantitative techniques, such as statistical analysis and numerical modeling, and qualitative techniques, such as content analysis and thematic analysis, will be needed. The data analysis will make it possible to spot trends, patterns, and connections between variables that may then be used to provide suggestions.

The data analysis will provide information on the current state of the protection system and the effectiveness of any suggested changes. The analysis' results will aid in the development of recommendations for improving the protection system's overall effectiveness. As a result of the research, effective protection measures that can protect the vital systems and operations of civil aviation businesses will be developed. The research will offer insightful information about the technological protection system of computer networks in civil aviation enterprises.

A combination of literature reviews, case studies, interviews, experiments, and data analysis approaches will be used to achieve the research aims and produce recommendations for improving the technological security of computer networks in civil aviation companies. With the help of the research, effective protection measures that can protect the vital systems and operations of civil aviation businesses may be developed. The research will offer insightful information about the technological protection system of computer networks in civil aviation enterprises.

CHAPTER 2
THEORETICAL PART

2.1. Key concepts and definitions related to technical protection of computer networks

There are a few basic terms and phrases that are crucial to comprehend when it comes to technological protection of computer networks. Some of the most crucial are listed below:

1. Cybersecurity: Protecting computer networks, systems, and data from unwanted access, theft, damage, or interruption is known as cybersecurity.

2. Threat: A threat to a computer network, system, or data is a potential risk to its safety or damage. Malware, hacking efforts, phishing scams, and social engineering are a few examples of risks.

3. Vulnerability: An attacker could take advantage of a weakness or hole in a computer network, system, or program to obtain unauthorized access or do harm.

4. Risk: The chance and potential consequences of a threat taking advantage of a vulnerability to hurt or damage a computer network, system, or data constitute risk.

5. Attack: An attack is a deliberate activity by an attacker to use a software, system, or network vulnerability to their advantage.

6. Firewall: Based on pre-established security rules, a firewall is a network security system that monitors and regulates incoming and outgoing network traffic.

7. An intrusion detection system (IDS) is a device that scans network traffic for indications of unauthorized access or activity and notifies administrators of potential dangers.

8. Encryption: To prevent unauthorized access or theft, encryption involves turning plain text or data into an encoded form.

9. Authentication: The process of confirming the identity of a user or device trying to access a computer network, system, or data is known as authentication.

10. Access control: Based on the user's identity and level of authorisation, access control is the process of limiting access to computer networks, systems, or data.

11. Multi-factor authentication: Before gaining access to a computer network, system, or data, users must first authenticate themselves using two or more different forms of identification (MFA).

12. Penetration testing: Penetration testing, sometimes called pen testing, involves evaluating software, systems, and computer networks for flaws and vulnerabilities by simulating an attack.

13. Security information and event management (SIEM): SIEM is a security tool that offers real-time monitoring of computer networks, systems, and data to spot security threats and incidents and take appropriate action.

14. Patch management: To address vulnerabilities and weaknesses, patch management entails routinely upgrading computer networks, systems, and software with the most recent security patches.

15. Cyber hygiene: The practice of upholding excellent cybersecurity habits and practices to safeguard computer networks, systems, and data against threats is referred to as cyber hygiene.

16. Social engineering: Attackers employ social engineering to manipulate and con people into disclosing private information or allowing access to computer networks, systems, or data.

17. Zero-day vulnerability: An attackable security issue in computer networks, systems, or software that is currently unknown to the vendor or the general public.

18. Antivirus software: By identifying and eliminating malware, antivirus software serves as a security solution for securing computer networks, systems, and data.

19. Data loss prevention (DLP): DLP is a security tool that aims to prevent data breaches by keeping an eye on and regulating the movement of sensitive data within computer systems, networks, and data storage devices.

20. Security audit: To detect and manage security risks and vulnerabilities, a security audit is a thorough review of computer networks, systems, and software.

21. Cyber threat intelligence (CTI) is the technique of gathering, evaluating, and sharing data on possible and existing cyber threats to assist organizations in proactively defending against them.

22. Network segmentation: This is the process of splitting a computer network into smaller subnetworks to increase security by limiting access to critical information and resources.

23. Incident response: The identification, containment, and mitigation of the effects of security incidents on computer networks, systems, and data constitute incident response.

Civil aviation businesses can improve their cybersecurity safeguards and safeguard their valuable assets and sensitive data by implementing these important ideas and definitions into their technical protection systems.

Relevance in the Context of Civil Aviation Computer Network Protection:

Given the vital nature of the industry and the potential repercussions of security breaches, protecting computer networks in the civil aviation sector is of the greatest significance. Following are some examples that will help you understand the importance of important terms and meanings linked to technological protection in this context:

Air traffic control, communication, navigation, and surveillance are just a few of the systems that rely on computer networks in civil aviation to operate safely and effectively. To maintain the integrity and dependability of these systems and reduce the danger of disruptions or accidents, it is imperative to ensure their protection.

Information that is sensitive and secret is handled via civil aviation networks, such as passenger records, flight schedules, and operational data. To safeguard passenger privacy, prevent unwanted access, and lessen the danger of data breaches or cyber-espionage, it is crucial to maintain the confidentiality and integrity of this data.

System resilience and continuity are improved by using technical security tools like firewalls, intrusion detection systems, and backup solutions in civil aviation. These precautions help to maintain network availability, reduce downtime, and guarantee uninterrupted operations by identifying and mitigating risks.

Compliance with Regulatory Requirements: The civil aviation sector is governed by stringent legal frameworks and cybersecurity compliance requirements. To fulfill these standards and exhibit a dedication to security best practices, concepts like vulnerability management, access control, encryption, and incident response are crucial.

Defense against Emerging Threats: A proactive and flexible strategy to technical protection in civil aviation is necessary given the changing threat landscape. It's essential to keep up with new threats, weaknesses, and attack methods in order to build efficient security controls and continuously enhance network security measures.

Stakeholders in the civil aviation sector can improve the security posture of their computer networks, reduce risks, and guarantee the safety and integrity of crucial systems and data by comprehending and putting into practice fundamental ideas linked to technological protection.

2.2. Methods of protecting computer networks

In order to secure the security and integrity of the network, protecting computer networks is a complex process that calls for a combination of technical and non-technical measures.

To help to safeguard computer networks against intrusion and attacks, firewalls are a crucial part of network security. A firewall essentially serves as a wall separating a private network from the internet or other public networks. Based on established security criteria, it monitors and filters incoming and outgoing network traffic, letting normal traffic flow through while blocking or warning on potentially harmful data.

There are several different kinds of firewalls, including cloud-based, software-based, and hardware-based firewalls. While each type has certain advantages and features of its own, they all contribute to the same objective—protecting network security.

Devices called hardware-based firewalls are positioned at the edge of the network, typically in the space between the public internet and the local network. They use specialized hardware to run, and their main job is to manage traffic that moves between the two networks. Hardware firewalls are especially helpful in large-scale deployments since they may offer a high level of security and performance.

On the other hand, software-based firewalls are placed on particular PCs or servers throughout the network. Instead of managing the entire network, they function by regulating the traffic that enters and exits a particular device. Although software firewalls may be less expensive than hardware-based firewalls, they might not offer the same level of performance or security.

A more recent sort of firewall that runs in the cloud rather than on-premises is called a cloud-based firewall. These firewalls can be quickly and readily deployed, and cloud providers often offer them as a service. For businesses searching for a scalable, manageable, and economical solution, cloud-based firewalls can be a desirable choice.

Regardless of the kind of firewall being utilized, they all share a few crucial characteristics. The capability to define security rules that specify what traffic is allowed and is banned from passing through the firewall is one of the most crucial features. The source and destination IP addresses, the kind of traffic, and the time of day can all be used as bases for these rules.

Additional security capabilities that firewalls can offer include intrusion detection and prevention, which can help in real-time attack detection and prevention. Additionally, they can be set up to record all network activity, which gives network managers useful data for analysis and problem-solving.

The need to balance usability and security is one of the difficulties with firewalls. Legitimate traffic may be prevented if security regulations are applied too strictly, which could interfere with regular business operations. However, if the guidelines are too lax, it can be simpler for attackers to access the network.

Firewalls can also provide users a false sense of security, which is a problem. Firewalls are a crucial part of network security, but they are not a cure-all. Attackers are always coming up with new strategies and methods to get around firewalls and other security measures. Firewalls should be used in addition to other security tools including antivirus software, intrusion detection and prevention systems, user education, and user awareness.

To sum up, firewalls are an essential part of network security. They act as a barrier, regulating traffic flow between a private network and the internet or other public networks. There are several different kinds of firewalls, including cloud-based, software-based, and hardware-based firewalls. Firewalls are a crucial part of network security, but they are not a cure-all. To defend against attacks and safeguard the integrity of your data, it's crucial to employ firewalls in conjunction with other security measures.

As part of its network security policy, the aviation sector employs intrusion detection and prevention systems (IDPS). Any contemporary cybersecurity plan must include intrusion detection and prevention systems (IDPS). By observing traffic, spotting and alerting on unusual behavior, and stopping attacks before they start, they assist in defending networks, systems, and applications from malicious attacks. We'll go deeply into IDPS in this post as we examine their main characteristics, subtypes, and advantages.

The acronym IDPS is what?

A security tool called an intrusion detection and prevention system (IDPS) watches over network and system activity to spot malicious activity and stop potential threats from jeopardizing a system or network. Intrusion detection and prevention systems (IDS and IPS) are combined into one system called an IDPS. While IPS takes action to stop the threat from happening, IDS looks for possible risks.

In order to detect potential security threats including malware, hacking attempts, and other malicious behavior, IDPS monitors and analyzes network traffic. It can examine traffic patterns, spot anomalies, and use this knowledge to find and stop threats. In order to identify and stop security problems, IDPS monitors network traffic and performs real-time analysis on it.

IDPS categories

Network-Based IDPS, Host-Based IDPS, Hybrid IDPS, and Cloud-Based IDPS are the four basic forms of IDPS.

Network-Based IDPS The Network-Based IDPS is installed at the network border and keeps an eye on all incoming and outgoing traffic. It examines network traffic and notifies administrators of any illegal access attempts or questionable activity. The first line of defense against threats and attacks from the outside world is frequently network-based IDPS systems.

IDPS Host-Based

On specific computers or servers, host-based IDPS is installed, monitoring system logs and activity to find and stop assaults on that host. Malware that has already infected the host system can be found and stopped using host-based IDPS, which can also recognize and stop harmful activity that takes place inside the host environment.

Fusion IDPS

A hybrid IDPS combines host-based and network-based IDPS. To offer thorough defense against security risks, it keeps an eye on network traffic and specific hosts. Larger businesses that need many layers of protection to safeguard their network and systems should use hybrid IDPS.

IDPS in the Cloud

The cloud-based IDPS is set up for protection of cloud-based services and applications. Platform as a service (PaaS), software as a service (SaaS), and infrastructure as a service (IaaS) attacks can be effectively detected and prevented using cloud-based IDPS.

Advantages of IDPS

Organizations can gain from IDPS in a number of ways, including:

Detecting and preventing threats

In order to identify and stop potential security risks before they might harm the network or systems, IDPS monitors network traffic.

Alerting in real-time

Real-time alerting from IDPS enables administrators to take immediate action in the event of a security threat.

Increasing Visibility

Administrators can spot potential security flaws and take immediate action thanks to IDPS's improved visibility into network activity.

Less downtime

By immediately identifying and thwarting attacks that can lead to network or system failures, IDPS can help decrease downtime.

A crucial element of any cybersecurity plan is IDPS. By delivering real-time alerts and improved visibility into network activities, it aids companies in identifying and preventing potential security issues. Network-based, host-based, hybrid, and cloud-based IDPS solutions are the four primary categories of these products. Depending on the requirements of the company, each type offers particular benefits. Deploying an IDPS solution is crucial to ensuring the security and integrity of organizational systems and data given the growing sophistication of cyber threats.

Another crucial component of network security in civil aviation is access control. Information security must include access control, which enables businesses to grant only authorized individuals access to critical information and resources. The process of providing or refusing access to resources or systems depends on the identity, function, and context of the individual making the request. Access to physical and digital resources, such as offices, computer networks, databases, and other IT systems, is controlled by access control systems.

The CIA triad, which stands for Confidentiality, Integrity, and Availability, includes access control as a key element. By preventing unauthorized individuals from accessing sensitive data, access control maintains confidentiality. By prohibiting illegal additions or modifications, access control also contributes to the preservation of the accuracy of data and systems. Finally, access control contributes to the availability of data and systems by ensuring that resources are only accessible to authorized users and thwarting malevolent activity such as denial of service assaults.

Physical access control and logical access control are the two basic divisions of access control systems. Systems for restricting access to actual locations, such as buildings, rooms, or other physical assets, are known as physical access control systems. On the other hand, logical access control systems are employed to regulate access to digital assets like computer systems, networks, or data.

Making sure that only people with permission can access a resource is the main goal of access control. The notion of least privilege, which states that a user is only given the minimal amount of access required to carry out their job functions, is something that access control systems are made to enforce. By preventing users from accessing resources they do not require to carry out their jobs, this lowers the possibility of unwanted access.

Access control systems come in a variety of forms, each with unique benefits and restrictions. The following are a few of the most popular kinds of access control systems:

Users can manage access to their own resources using Discretionary Access Control (DAC), a sort of access control system. Each resource in a DAC system has an owner who is in charge of controlling access to it. Because users have total authority over their resources and access rights are not centralized, this sort of access control is not very secure.

Mandatory Access Control (MAC): Compared to DAC, MAC is a sort of access control system that offers a higher level of protection. In a MAC system, the system's enforcement of a set of predetermined rules and policies governs access to resources. Users are not permitted to alter these policies, which are established by a system administrator. In settings requiring high levels of security, such governmental and military institutions, MAC systems are frequently employed.

RBAC is a form of access control system that gives access to resources based on a user's function within an organization. Each user is given a unique role, and based on the privileges attached to that position, access to resources is determined. RBAC systems are frequently employed in large organizations with a high number of users and varying levels of access.

Access control systems known as Attribute-Based Access Control (ABAC) provide users access to resources based on their attributes, such as their job title, department, or location. Since access can be granted based on a variety of attributes, ABAC systems are more versatile than RBAC systems.

Access control lists (ACLs), smart cards, and biometric authentication are just a few of the technologies that can be used to construct access control systems. In contrast to smart cards, which store user credentials like usernames and passwords, biometric authentication employs distinctive bodily attributes to identify users, such as fingerprint or iris scans.

Access control is a crucial component of information security that enables businesses to safeguard their assets from unauthorized access. Access control systems, which can be implemented using a range of technologies, are used to regulate access to both physical and digital resources. Organizations can lower the risk of security breaches and data loss by installing access control systems to make sure that only authorized individuals are permitted access to sensitive data and systems. In order to make sure that the system is effective at enforcing access restrictions and preventing illegal access, it is crucial to choose the appropriate type of access control system depending on the needs and requirements of the company. Access control systems must be regularly monitored and audited to make sure they are operating properly and that access privileges are current and appropriate for each user. Access control should be implemented as part of a comprehensive security plan to secure an organization's most important assets because it is a crucial feature of any information security program.

Cyber-attacks can target the sensitive and confidential data sent over the network, such as customer information, banking information, and trade secrets. Businesses and individuals are at danger as a result of the constant development of new methods by hackers and cybercriminals to intercept and steal data. Data encryption has developed into a crucial technique for network security in order to counter these dangers.

Describe encryption.

Encryption is the process of transforming plain text into ciphertext, an unintelligible format. The method encrypts the data using a key and a mathematical algorithm. The ciphertext is incomprehensible to anyone who intercepts it since only those with the right decryption key can decode it and read and comprehend it.

Symmetric and asymmetric encryption are the two main categories of encryption methods. The same key is used for encryption and decryption in symmetric encryption. A public key and a private key are used in asymmetric encryption for encryption and decryption.

Synchronous encryption

A popular encryption technique for network data security is symmetric encryption. Symmetric encryption encrypts and decrypts data using the same key shared by the sender and recipient. The confidentiality and integrity of the data are guaranteed by maintaining the encryption key's secrecy between the sender and the recipient.

The majority of the time, symmetric encryption methods are quicker and use less resources than asymmetric encryption techniques. The security of the key must be ensured, though, because it is used for both encryption and decryption. The data is exposed to attack if the key ends up in the wrong hands.

Asymmetric Cryptography

Asymmetric encryption, commonly referred to as public-key encryption, encrypts and decrypts data using two keys: a public key and a private key. While the private key is kept a secret, the public key is accessible to everyone. Only the private key that corresponds to the public key can decode material that has been encrypted with it.

Because the private key is kept secret, asymmetric encryption is more secure than symmetric encryption. As a result, it is more challenging for attackers to obtain the key and decrypt the data. However, compared to symmetric encryption techniques, asymmetric encryption algorithms are typically slower and use more resources.

Network Ensurance

Data transmission over a network is encrypted during the network encryption procedure. Data sent across wireless networks, the internet, and other network connections are included in this. Data confidentiality and integrity are guaranteed by network encryption, shielding it from theft and eavesdropping.

There are numerous methods for achieving network encryption, including the use of VPNs and the Secure Sockets Layer (SSL) protocols. Through an untrusted network, VPNs enable a secure connection between two or more devices. SSL protocols encrypt data exchanged between a web server and a web browser, preventing the interception of sensitive data like credit card numbers.

Optimal Network Encryption Techniques

There are various recommended practices that should be followed to guarantee the security of network data:

Use robust encryption methods: To ensure that the data is appropriately safeguarded, use robust encryption algorithms like Advanced Encryption Standard (AES).

Implement key management: To secure the safety of the encryption keys, implement a key management system. Access to the keys should be limited, and keys should be replaced frequently.

Use SSL/TLS to encrypt online traffic: online traffic should be encrypted using SSL/TLS protocols. This makes sure that private information, including login credentials and payment card information, cannot be accessed.

Use VPNs to enable remote access for network resources in a secure manner. This guarantees the encryption and security of data being transported between remote devices and the network.

Test encryption frequently: Test encryption frequently to make sure it is functioning properly and adhering to the most recent security guidelines.

A crucial element of network data security is encryption. It makes sure that private information sent over the network is shielded against theft and eavesdropping. Symmetric and asymmetric encryption are the two main categories of encryption techniques, and each has advantages and disadvantages. VPNs and SSL protocols can be used to implement network encryption, and a number of recommended practices should be followed to guarantee the security of network data. Organizations can help safeguard their data and guarantee the confidentiality and integrity of their network connections by deploying robust encryption techniques and routinely testing encryption.

Sustaining safe and secure air travel depends critically on the protection of computer networks in civil aviation. Computer networks are protected using a variety of crucial techniques, including firewalls, intrusion detection and prevention systems, access control, data encryption, and software updates. To remain ahead of developing cyber dangers, it is crucial to remember that no security solution is flawless, thus security systems must be constantly monitored and updated.

2.3. Technical protection systems for computer networks

Computer network technical protection measures are essential for preserving the availability, confidentiality, and integrity of data and resources. To identify, stop, and mitigate possible cyber attacks, these systems use a variety of techniques, technologies, and procedures. Here are a few often employed technical fences for computer networks:

Monitoring and logging systems for computer networks are essential components of the technological protection systems that are used for these networks. These systems function by monitoring and analyzing network traffic, which gives enterprises insights into the activity of their networks, identifies potential security vulnerabilities, and makes it easier to respond to incidents and conduct forensic investigations. Let's dig a little deeper into the inner workings of network monitoring and logging systems, along with some concrete instances of well-known software options.

Taking a Snapshot of the Network Activity Network monitoring systems take snapshots of the network activity using a variety of techniques, including port mirroring, network tapping, and packet sniffing, among others. As an illustration, Wireshark is a popular example of a network protocol analyzer that gives administrators the ability to capture and inspect packets in real time. It is compatible with a wide variety of network interfaces and provides extensive information about packets that have been collected.

After the network traffic has been captured, the network monitoring systems then analyze the packets to extract information that is pertinent to the situation. Decoding the packet headers and payloads is required for this analysis so that we can understand the source and destination IP addresses, ports, protocols being used, and the contents of the packets. Tools such as Tcpdump and Tshark give command-line interfaces for the study of packets and offer various filtering options to focus on particular types of network traffic that are of interest.

Event Detection and Alert Generation: Network monitoring systems utilize complex algorithms and predefined rules to analyze network data in order to identify events and anomalies. For instance, intrusion detection systems (IDS) and intrusion prevention systems (IPS) monitor network traffic for known attack patterns and generate alerts whenever suspicious activity is discovered. Snort is a well-known open-source intrusion detection and prevention system (IDS/IPS) that may be set up to identify and counteract a wide variety of network-based assaults.

Keeping a track and Storing Information Network monitoring systems keep a track of network events, activities, and alarms for the purpose of conducting audits and doing future analyses. The logs record pertinent information such as timestamps, source and destination IP addresses, and descriptions of events that were seen. Splunk and ELK (Elasticsearch, Logstash, and Kibana) are two popular log management technologies that enable businesses to gather, store, and analyze network logs from numerous sources. This gives businesses a centralized picture of the actions that occur on their networks.

Real-time Monitoring and Visualization: Network monitoring systems typically include real-time monitoring and visualization capabilities to give administrators an accurate picture of how their networks are operating at any given time. Solutions such as Nagios and PRTG Network Monitor offer comprehensive monitoring tools, such as dashboards, graphs, and alarms that can be customized. These features enable administrators to monitor the health of a network and respond quickly to any problems that may arise.

Compliance and Reporting: Compliance requirements and reporting needs can be supported by network monitoring and logging systems since these systems generate thorough reports based on the activities and events that occur on the network. These reports can provide businesses with the assistance they need to establish compliance with security policies, legal obligations, and industry standards. For instance, the compliance reporting features provided by SolarWinds Network Performance Monitor can aid enterprises in meeting the requirements imposed by regulatory authorities.

Organizations are able to proactively detect and respond to security risks, enhance network performance, and maintain compliance with industry laws when they utilize monitoring and logging systems for their networks and leverage their capabilities. Essential functionalities such as real-time monitoring, packet analysis, event detection, alarm generation, logging, and reporting are all offered by these systems. It is imperative that businesses choose the most suitable network monitoring and logging solutions based on the requirements and necessities that are unique to their corporation.

The use of antivirus and anti-malware software is an essential part of any technological protection solution for computer networks. These software solutions are extremely important in avoiding, identifying, and eliminating risks posed by malicious software, which can put the safety and integrity of computer networks at risk. Let's investigate the inner workings of anti-malware and antivirus software, along with some real-world instances of well-known programs that fall into this category.

Detection of Malware: Anti-malware and antivirus software utilize a wide variety of detection techniques in order to discover and recognize potential malware threats. Methods such as behavior-based detection, signature-based detection, heuristic analysis, and machine learning algorithms are included in these strategies.

Signature-based detection is an approach that compares the coding patterns and attributes of files to a large database that contains known virus signatures. In the event that a match is discovered, the program will label the file as being malicious. Software such as Norton Antivirus, McAfee Antivirus, and Avast Antivirus are all examples of programs that utilize this method.

The behavior-based detection method is a strategy that focuses on the identification of suspicious behaviors performed by software, which may signal the presence of malicious activities. The program keeps a close eye on the processes, file system modifications, network connections, and other activities across the system in order to identify odd behavior patterns that are characteristic of malware. Antivirus software such as Bitdefender and Kaspersky employ a technique known as behavior-based detection.

Heuristic analysis is a technique that includes looking at the behaviors and architecture of files to find potentially dangerous patterns or actions. In order to detect potentially malicious code snippets or sequences, the program employs a set of rules and algorithms. Antivirus software such as ESET NOD32 Antivirus is an example of a piece of software that use heuristic analysis to identify malicious software.

Algorithms that learn from their environment Machine learning algorithms are used by advanced anti-malware solutions to evaluate enormous quantities of data in order to understand patterns of known malicious software and the behaviors it exhibits. Because of this, they are able to identify new and previously undiscovered forms of malware based on the knowledge they have gained. Examples of this include Windows Defender, which has machine learning capabilities built right in, and Malwarebytes, which has increased threat detection thanks to the use of machine learning.

Removing Malware and Placing It in Quarantine When anti-malware and antivirus software detects a malware threat, it immediately takes action to either delete or place the infected files in quarantine. They either remove the harmful code from the infected files or place them in an environment that is safe in order to prevent any further damage from occurring. Quarantined files are frequently encrypted or moved to a secure location, both of which ensure that they cannot cause any damage to the system.

Real-Time Protection Real-time protection is provided by anti-malware and antivirus software, which does this by monitoring the activity of the system and the data it contains in real time. They do thorough checks on all incoming and outgoing network traffic, email attachments, downloaded files, and visited websites in order to eliminate any possibility of malicious software sneaking into the system. This round-the-clock monitoring helps to spot potential dangers and shut them down before they can do any damage.

Automatic Updates In order to tackle the ever-evolving dangers posed by malware, anti-malware and antivirus software automatically update their signature databases of malware, detection algorithms, and system vulnerabilities on a regular basis. These upgrades guarantee that the software is always up to date with the most recent dangers and is able to successfully identify and defend against new strains of malicious software. It is absolutely necessary to utilize automatic updates in order to keep the program functioning at its optimal level.

extra Protection Many anti-malware and antivirus software packages have extra protections, which can be activated if a threat is detected. Firewall protection, web surfing protection, email scanning, analysis of browser extensions, and vulnerability assessments are a few examples of the functions that may be included here. Avira Antivirus, for instance, offers online protection and filters harmful websites, whereas Trend Micro Security offers email scanning and attachment screening.

It is critical for businesses to select anti-malware and antivirus software solutions that come from trustworthy companies and can be relied upon. These solutions should also be routinely updated, be capable of identifying threats in their entirety, and have extra features that can be used to improve overall system security. The examples of well-known antiviral software that have been offered in this response are shown below;

however, there are many additional solutions on the market that provide functionality that is comparable to that of the examples presented.

Although anti-malware and antivirus software are important components of a technical protection system, they should be supplemented with additional security measures such as regular system updates, strong password policies, user awareness training, and secure network configurations to ensure comprehensive protection against cyber threats.

When it comes to protecting the authenticity and accessibility of data in computer networks, solutions for data backup and disaster recovery play an extremely important part. These solutions are intended to prevent the loss of data and make it easier to recover essential information in the event that unforeseen accidents or natural catastrophes occur. Let's look into the inner workings of data backup and disaster recovery solutions, along with some instances of well-known popular systems that fall into this category from the real world.

Backup of Data: Creating copies of vital data and storing them in a different place or media is what is meant by "backing up" your data. The basic objective of data backup is to produce a duplicate of the data that is both trustworthy and up to date. This copy may then be put to use for data recovery in the event that the data in its original form is corrupted or rendered inaccessible.

There are many different ways to back up one's data, including the following:

Full Backup is a process that involves making a complete copy of all of the data, which includes the files, directories, apps, and settings for the system. Although it might be time-consuming and calls for a substantial amount of storage space, it does give a full backup.

Only the modifications that have been made since the most recent full backup are stored using the incremental backup approach. When compared to complete backups, it cuts down on the amount of time needed for backups and the amount of storage space required, but the restoration procedure may take longer since numerous backups need to be consolidated.

A differential backup, sometimes known as an incremental backup, is very similar to an incremental backup in that it only preserves the changes that have been made since the most recent complete backup. However, it does not affect the prior differential backups, which enables the restoration process to go more quickly and with fewer complications.

Recovery from Disaster: Recovery from disaster refers to the methods and tactics that are followed in order to restore information technology systems, applications, and data in the aftermath of a disruptive event such as a natural catastrophe, hardware failure, or cyberattack. It seeks to shorten the amount of time that important processes are interrupted for as little as feasible.

The following are important elements that make up a disaster recovery solution:

Recovery Point Objective (RPO) is a term that describes the maximum amount of data loss that is considered acceptable during a period of time. It establishes how frequently data backups need to be carried out in order to satisfy recovery goals.

Recovery Time Objective (RTO) is the predetermined amount of time within which all of a company's operating systems and data must be restored following a catastrophic event. It establishes the maximum amount of downtime that is acceptable for company operations.

Examples from Everyday Life:

Backup & Replication by Veeam: Veeam is a company that offers complete data protection and disaster recovery solutions for virtual, physical, and cloud-based settings. Veeam Backup & Replication. It supports automatic backups, replication, fast recovery, and granular file-level recovery as some of its available options.

A unified backup and recovery solution is provided by Acronis Cyber Backup, which is available for a wide variety of IT settings. It offers features like as backups based on images, configurable recovery options, protection from ransomware, and safe cloud storage.

Complete Backup & Recovery from Commvault: Commvault provides a unified backup and recovery platform that is compatible with a wide variety of data sources and operating environments. Deduplication, snapshot management, data archiving, and automated disaster recovery are some of the features that are included in this solution.

Veritas NetBackup is an enterprise-level backup and recovery solution that is meant to safeguard large-scale and diversified IT systems. Veritas NetBackup was developed by Veritas Software. It provides functionality such as data deduplication, snapshot management, interaction with the cloud, and automated recovery operations.

These are some examples of data backup and disaster recovery systems that have a good reputation and are used extensively in the business. However, it is essential to do an analysis and select a solution that is compatible with the organization's particular requirements, scope, and financial constraints.

It is essential to put in place comprehensive data backup and disaster recovery solutions in order to guarantee company continuity, reduce the likelihood of experiencing data loss, and cut down on the amount of time lost due to system failures or other unanticipated occurrences. When such solutions are incorporated into the technical protection system, businesses are able to secure their essential data assets and make it easier to retrieve data quickly in the event that it is necessary to do so.

Patch management systems are a key part in the process of ensuring that computer networks continue to function properly and remain secure. These solutions assist companies in maintaining the most recent versions of their software and operating systems by applying patches and updates that have been made available by software suppliers. In this part, we will investigate the inner-workings of patch management systems and present concrete illustrations of well-known products now available on the market.

The process of patch management consists of:

Identification of Patches In order to determine which patches and updates are now available, patch management systems perform regular scans of the websites of software providers, as well as security advisories and other reliable sources. They investigate the vulnerability or flaw that the patch is intended to fix and decide whether or not it is relevant to the environment in which the company operates.

Assessment of Patches: Once patches have been found, they are put through an evaluation procedure to determine the impact that they will have on the systems used by the company. This involves identifying the severity of the vulnerability, whether or not the patch is compatible with the software and settings that are already in place, and the possible hazards involved with deploying the patch.

Deployment of fixes: After the assessment, the fixes that have been authorized are delivered in a controlled way to the systems that have been compromised. Patch management systems offer automated processes for installing patches, which may include the capability of scheduling the distribution during non-peak hours, spreading updates across various systems, and ensuring that successful installs have taken place.

Testing of Patches: Before being deployed, patches may be put through testing in a confined environment to ensure that they do not cause any incompatibilities or problems with the currently installed software or with the settings of the system. Testing helps reduce the likelihood of undesirable outcomes being brought about by the installation of a patch by identifying and removing potential problems.

Verification of Patches After patches have been distributed, the patch management system checks to ensure that they were successfully installed and looks for any potential problems or conflicts that may have arisen. It is also possible that it may give reporting capabilities, which will track patch compliance across the network and indicate systems that need more care.

Microsoft Windows Server Update Services (WSUS): WSUS is a patch management system that is especially built for use with Microsoft products. It is quite popular and has a wide range of applications. It gives businesses the ability to centrally manage the distribution of Microsoft product updates, security patches, and service packs across all Windows-based computers in their company.

Organizations are in a better position to proactively fix software vulnerabilities, protect themselves against possible threats, and maintain the stability and security of their computer networks when they have a strong patch management system in place. Maintaining a secure and robust network infrastructure requires performing routine patching, which is an essential component.

2.4. Specifics of technical protection of computer networks in civil aviation

Because of the extremely important nature of aviation operations and the possible dangers that are linked with cyber attacks, the technological security of computer networks in civil aviation needs very particular considerations to be taken into account. Let's have a look at some of the most important aspects of the technological safeguarding of computer networks in the civil aviation industry.

Compliance with rules: The industry of civil aviation is subject to a variety of rules and standards on information security and cybersecurity. These regulations and standards must be followed. The standards for securing computer networks and sensitive information are established by these rules, such as those that are defined in ICAO Annex 17, and the guidelines that are provided by national aviation authorities. In order to assure compliance with these rules and to continue ensuring the safety and security of aviation operations, technical protection measures need to be aligned with them.

Protection of Operational Systems Computer networks in civil aviation comprise a broad variety of operational systems. Some examples of these systems are air traffic management, flight planning, aircraft communication systems, weather monitoring, and maintenance systems. These systems are very necessary to ensure that aviation services are carried out in a reliable and effective manner. It is necessary to carefully develop technical protection measures in order to secure these operating systems from illegal access, data breaches, and disturbances that may have an effect on flight safety.

Defense-in-Depth Strategy: A defense-in-depth strategy is frequently utilized in the process of providing technological protection for computer networks used in civil aviation. In order to achieve this, many layers of security controls need to be implemented so that the security posture may be both strong and resilient. Firewalls, intrusion detection and prevention systems, network segmentation, access restrictions, encryption, and strong authentication procedures are examples of the types of layers that may be included in this category. This technique, which consists of several layers, serves to reduce the risk of possible vulnerabilities and assures that even if one layer is breached, other levels will continue to offer security.

Threat Intelligence and Risk Assessment: Organizations that deal with civil aviation need to have a thorough comprehension of the ever-changing cyber threat landscape. Monitoring threat intelligence sources on a consistent basis, such as platforms designed specifically for the exchange of cybersecurity information in the aviation sector and industry alerts, assists in identifying new threats and vulnerabilities. Organizations are able to prioritize and effectively allocate resources for the implementation of technical protective measures based on the identified risks when they conduct risk assessments that are particular to the aviation environment and are specific to the aviation environment.

Response to Incidents and Maintaining Business Continuity: Despite the implementation of preventative measures, accidents and breaches of security can still take place. As a result, businesses involved in civil aviation need to have solid procedures for responding to incidents and strategies for maintaining business continuity. These plans specify the measures that are to be performed in the event that there is a breach in security, including the containment of the breach, investigation of the breach, recovery of impacted systems, and restoration of those systems. For the purpose of assisting in the discovery and resolution of incidents, technical protection systems should integrate methods for the logging and monitoring of network activity.

Training and awareness are two of the most important aspects of the technological protection of computer networks. Human factors play a pivotal part in this protection. It is very necessary to give workers, contractors, and stakeholders involved in civil aviation operations with ongoing training and awareness programs on a consistent basis. This training has to include subjects like the best practices for cybersecurity, how to recognize phishing efforts, how to use secure systems, how to manage passwords, and how to report incidents. It is possible for organizations to improve the general level of technical protection provided by computer networks if they raise awareness of the issue and promote a culture that is security conscious.

These particulars bring to light the one-of-a-kind concerns and difficulties that are inherent in the process of providing technological protection for computer networks in civil aviation. The aviation sector has the ability to improve information security, protect vital systems, and reduce the potential hazards caused by cyber attacks if it addresses these issues and puts suitable measures into place.

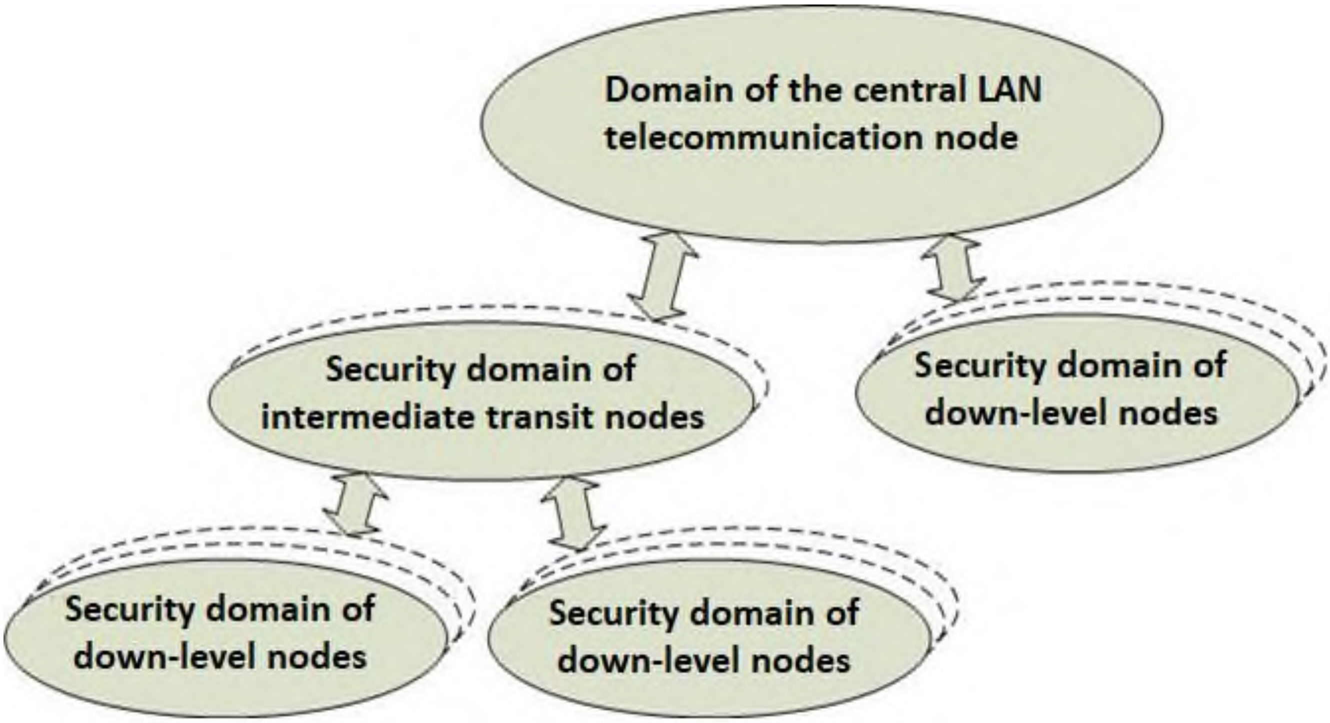
CHAPTER 3
PRACTICAL PART

3.1. Analysis of the existing technical protection system for computer networks in civil aviation

While doing an analysis of the present technical protection system for computer networks in civil aviation, one of the tasks that must be completed is an evaluation of the efficiency and sufficiency of the measures that are currently in place to secure the network infrastructure, data, and systems that are employed by civil aviation businesses. In order to strengthen the overall security posture, the mission is to locate any potential vulnerabilities, places of weakness, or problem spots that need to be fixed.

In most cases, the analysis will involve the following procedures:

Assessing the existing security policies, guidelines, and procedures linked to network protection inside civil aviation firms is one of the tasks that will be covered in this review of security policies and procedures. Examining rules pertaining to access control, data encryption, incident response, and disaster recovery is an important part of this process.


Domain of the central LAN telecommunication node
Security domain of intermediate transit nodes
Security domain of down-level nodes
Security domain of down-level nodes
Security domain of down-level nodes

General structure of the information protection system at the Airport's local network

An evaluation of the existing network infrastructure, including all routers, switches, firewalls, and other network devices is referred to as a network infrastructure assessment. Performing this step requires locating any pieces of equipment that are out of date or vulnerable, as well as any misconfigurations or potential failure points that could undermine the security of the network.

Assessment of Vulnerability: The process of conducting an exhaustive vulnerability assessment of the computer network in order to locate any potential vulnerabilities and security holes. This may involve employing tools for vulnerability scanning or engaging in penetration testing to replicate real-world attack situations. Alternatively, this may involve both.

Threat Detection and Intrusion protection: Evaluating the efficiency of already-installed monitoring, protection, and detection systems for threats and intrusions. This includes reviewing the deployment and configuration of security solutions such as antivirus software, intrusion detection and prevention systems (IDPS), and security information and event management (SIEM) tools.

Evaluating the data protection methods that are currently in place, such as data encryption, access controls, and frequent backup procedures, is an important part of data protection and backup. This includes assessing backup and recovery techniques to verify that vital data can be accessed and that it retains its integrity.

Evaluation of User Awareness and Training: Evaluating the amount of user awareness and training regarding network security practices and policies. Examining the efficiency of training programs, security awareness campaigns, and user compliance with security protocols is a necessary step in this process.

Compliance and Regulatory Requirements: Ensuring that the existing technical protection system is in alignment with the relevant compliance regulations and industry best practices, such as those defined by regulatory bodies such as the Federal Aviation Administration (FAA) or the International Civil Aviation Organization (ICAO).

Analysis of the Findings and Recommendations for Gaps Conducting an analysis of the results of the assessment in order to identify any gaps or areas in which changes are required. This involves putting forward proposals for improving the technological protection system, such as establishing extra security controls, upgrading network devices, or improving employee training programs.

When conducting an assessment of the present technological protection system for computer networks in civil aviation, it is necessary to take an extensive and methodical approach in order to successfully detect weaknesses and devise solutions for such flaws. It contributes to the establishment of a comprehensive security posture that protects vital infrastructure and data within civil aviation businesses.

3.2. Development and proposal of improvements for the technical protection system for computer networks in civil aviation

3.2.1. Simulation environment

In order to create a protection system for computer networks that is both efficient and reliable, it is necessary to use an integrated strategy that makes use of multiple protection approaches concurrently. In the modern digital landscape, relying on a single security mechanism is frequently insufficient to manage the myriad of dangers that computer networks must contend with on a daily basis. Organizations have the ability to improve their overall security posture and better protect their important systems and data if they implement a defense strategy that is composed of multiple layers.

Packet tracer is a program that can be utilized to humanity in order to simulate and test a local area network. Packet Tracer is a powerful tool for simulating virtual networks that gives users the ability to build and test their own virtual networks.

The following is a list of some of the benefits of utilizing Packet Tracer:

Packet Tracer offers a simulated environment for network design, configuration, and troubleshooting with its Network Simulation feature. Users are given the ability to construct and alter network topologies, setup devices, and simulate network traffic, which assists in the learning of various networking concepts and the practice of those ideas.

Packet Tracer comes equipped with a wide selection of virtual Cisco devices, including routers, switches, firewalls, and servers. Users are given the ability to simulate and test a variety of network scenarios without the requirement of physical hardware thanks to the fact that these virtual devices may be readily added to the network architecture.

Built-in Networking Tools Packet Tracer comes equipped with a variety of built-in networking tools, including ping, traceroute, and traffic generators, which enable users to test connectivity, diagnose network problems, and assess network performance while operating in a simulated environment.

Educational Resource: Due to the fact that it offers a functional environment for students to gain practical experience through hands-on training, Packet Tracer is frequently utilized in networking classes and certifications. Students are able to obtain significant experience in the design, configuration, and troubleshooting of networks in an environment that is secure and controlled thanks to this activity.

Collaboration: Packet Tracer users are able to work together on projects by sharing their network topologies and configurations with one another. This feature makes it easier to complete group projects and improves remote learning by allowing numerous users to collaborate simultaneously on the same network design.

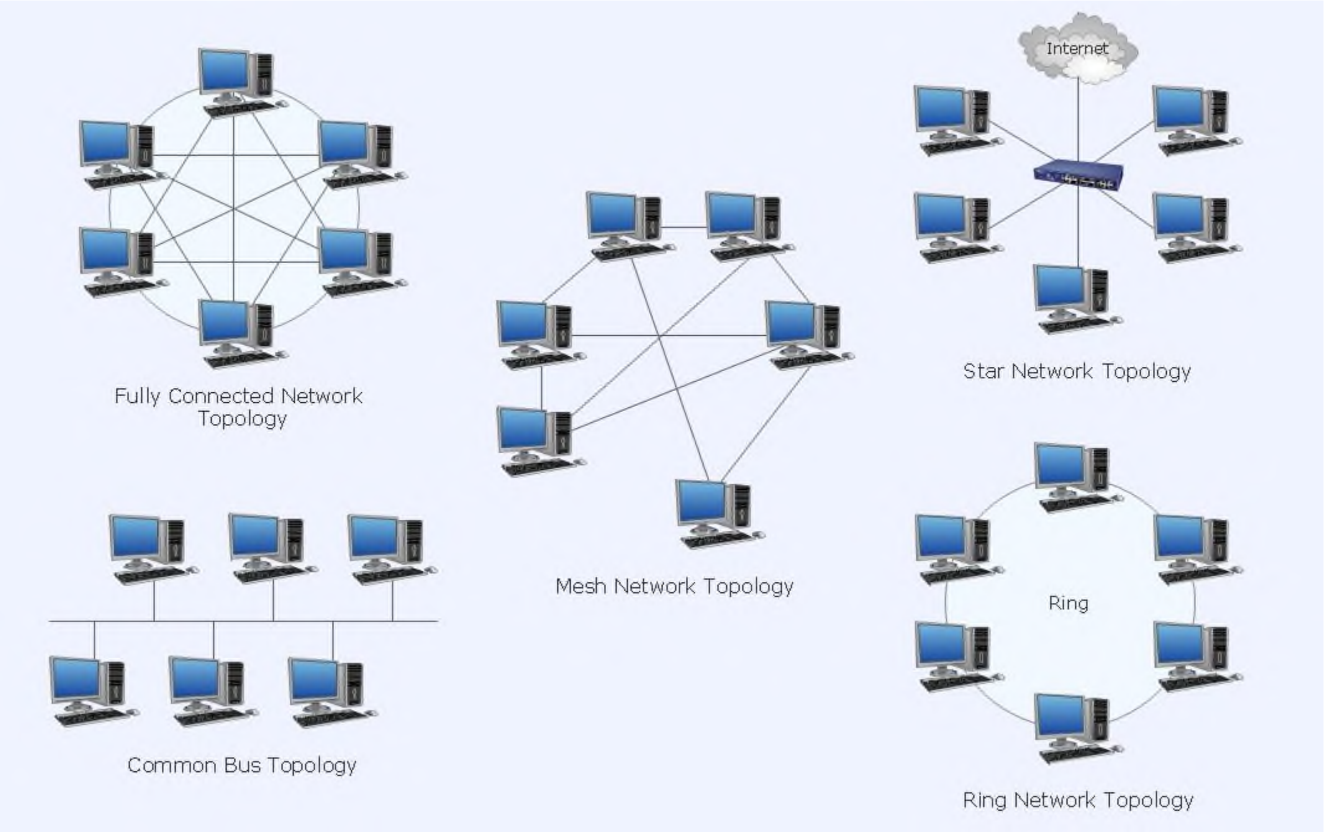
Packet Tracer is a free piece of software that provides a solution that is both cost-effective and efficient for the simulation and learning of network protocols. It eliminates the need to make an expensive initial investment in physical network equipment in order to train and experiment with it.

In general, Packet Tracer is a sophisticated tool that can be used for network simulation and learning. It offers a platform that is both practical and accessible for network design, configuration, and troubleshooting.

3.2.2. Network topology

Initially, network topology must be determined. In computer networks, network topology refers to the architecture or structure of the network. Different network topologies have their own efficiency, scalability, and security advantages and disadvantages. The choice of network topology is influenced by a number of variables, including network size, user requirements, and available resources.

Here are examples of prevalent network architectures:



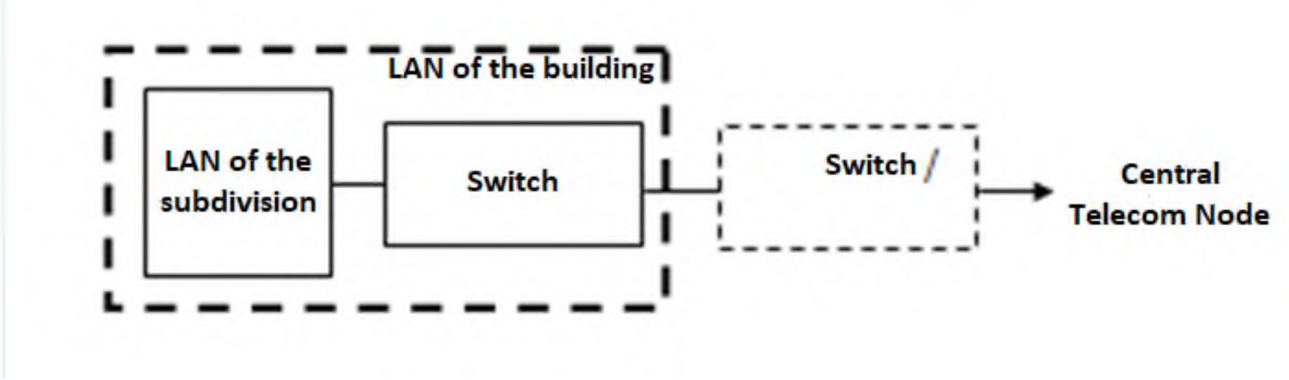
Structure scheme of logical topologies.

Each device in a bus topology is connected to a single cable known as a bus. The bus transmits data between ends, and each device listens to its own data. This is a simple and frugal topology, but it is collision-prone and insecure.

In a star topology, all devices are connected to a central node or switch. Each device has its own dedicated connection to the hub, allowing for direct data transmission between the device and the hub. It offers superior performance, scalability, and defect tolerance compared to bus topology. It is extensively used in contemporary networks and is regarded as more secure because the failure of a single device does not compromise the entire network.

In a ring topology, devices are connected in a closed cycle and data is transmitted in a single direction along the ring. Each device functions as a repeater by amplifying and transmitting the signal to the following device. Ring topologies offer superior performance and are simple to deploy, but the failure of a single device can disrupt the entire network.

Mesh Topology: In a mesh topology, each device is connected to every other device on the network, resulting in a network that is completely interconnected.



Structural scheme of a subnet of a corporate computer network

Multiple data paths provide the greatest level of redundancy and fault tolerance. Mesh topologies are extremely robust, but their implementation can be difficult and costly.

The most efficient and secure network topology is determined by the network's specific requirements and constraints.

Combination of several topologies will provide a high level of security if access control and security measures such as firewalls and intrusion detection systems are properly implemented.

3.2.3. Network nodes organization

The organization of network components, as well as the sequence in which network nodes are placed, is an important consideration for the overall operation and safety of the network. The location of network nodes can have an effect on aspects such as the performance, the flow of traffic, the level of security, and the capacity to administer the network.

The following equipment has been used:

Cisco ASA 5506-X: is a next-generation firewall. It offers advanced security features such as stateful packet inspection, intrusion prevention system (IPS), VPN capabilities, and application visibility and control. The 5506-X provides a combination of firewall, VPN, and routing functionalities, making it suitable for securing network traffic and protecting against various threats.

Cisco ISR 4331: is a branch router designed for medium-sized and large-sized branch. It offers a wide range of features, including advanced security, WAN optimization, application visibility, and integrated services. The ISR 4331 supports multiple WAN connections, such as Ethernet, T1/E1, and LTE, providing flexible connectivity options.

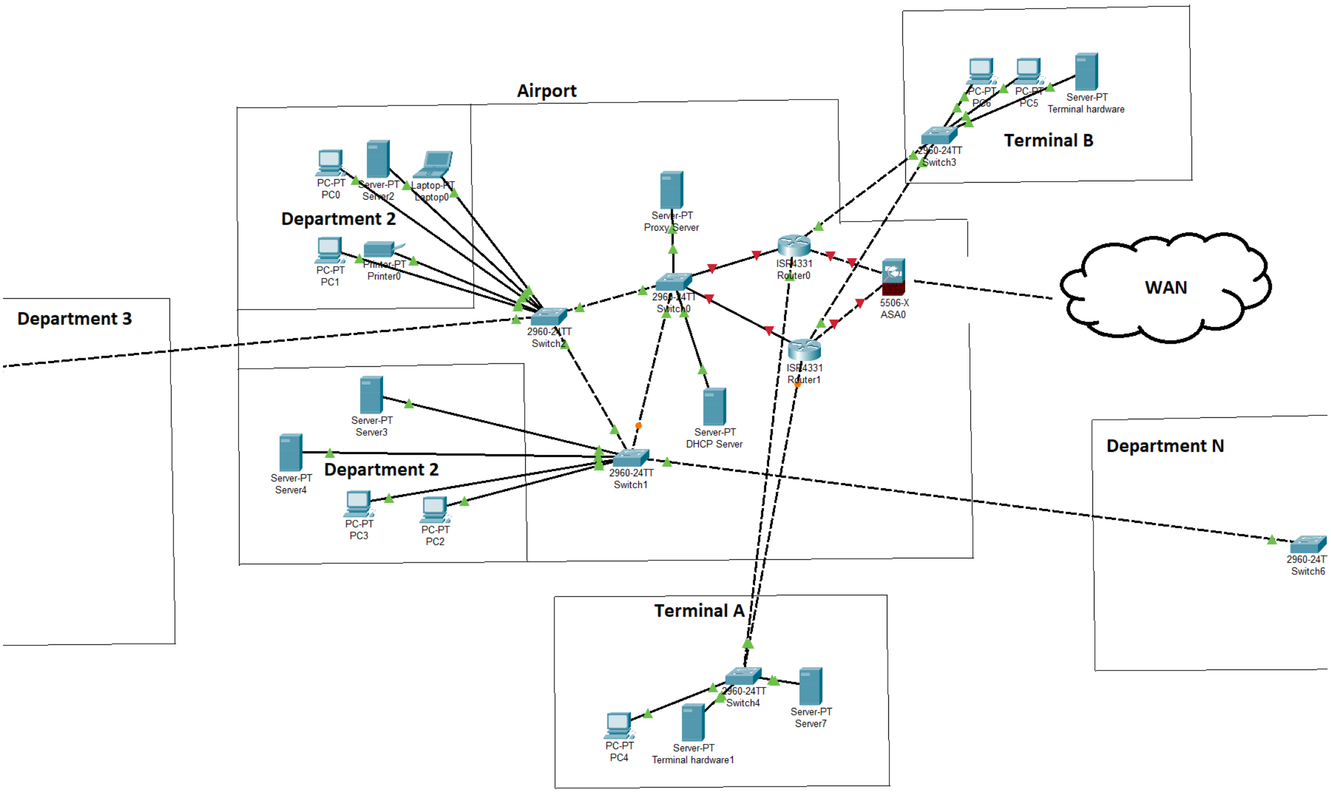
Cisco Catalyst 2960: is a family of fixed-configuration Ethernet switches designed for medium-sized networks. These switches offer enterprise-class features, including high-performance switching, VLAN support, quality of service (QoS), and security features. The Catalyst 2960 switches are available in various models with

different port densities and uplink options, providing flexibility for network deployments.

All network nodes are connected with CAT 6

Ethernet cable of the category 6 (often abbreviated Cat 6) is a type of twisted pair cable that is frequently used for making connections to Ethernet networks. In comparison to preceding cable classifications, it is constructed to enable a greater bandwidth and a more rapid data transfer rate.

Cat 6 cables are distinguished by their use of four separate pairs of copper wires and RJ-45 connectors as their points of termination. When used over shorter distances, these cables are capable of supporting Gigabit Ethernet (1000BASE-T) and even 10 Gigabit Ethernet (10GBASE-T). Cat 6 cables may be up to 100 meters (328 feet) in length if they are used for lesser data speeds, while the maximum length for 10GBASE-T is just 55 meters (180 feet).



Logical network topology of the airport

When it comes to connecting interfaces, Cat 6 cables are compatible with a wide array of networking equipment, including switches, routers, network adapters, and patch panels. The majority of networking equipment come equipped with conventional Ethernet ports, which are compatible with the RJ-45 connection used on Cat 6 cables.

The configuration of a firewall, router, switch, and proxy, in that order, is often regarded as optimal for a number of reasons:

In terms of network security, the inspection and filtering of incoming and outgoing network traffic based on specified security policies is made possible when the firewall is placed at the beginning of the sequence. Protecting the network against unauthorized access, hostile assaults, and potential security breaches is the primary function of the firewall, which serves as the network's first line of defense.

Traffic Routing: The router is the component that follows after the firewall and is responsible for the traffic routing within the network. It does this by determining the route across networks that is the quickest and most effective way for data packets to transit. This keeps traffic flowing smoothly and ensures that it reaches its intended destinations. The router contributes to the overall improvement of the network's performance and connection.

The switch is in charge of connecting devices that are part of the local network and is responsible for network segmentation. Putting it after the router enables network segmentation and the development of independent network segments, such as Virtual Local Area Networks (VLANs). VLANs are an abbreviation for "virtual local area networks." This segmentation strengthens the network's security by isolating and confining any possible risks, hence reducing the effect those threats have on the overall network.

Access Control and Caching: The proxy server is positioned after the switch and offers extra safety measures and functionality. It also caches information for faster access. It facilitates access control, content filtering, caching, and overall enhanced speed by acting as a middleman between client devices and the internet. The proxy server contributes to the enforcement of policies, helps limit access to particular websites or material, and can provide an additional layer of security against harmful activity.

This combination contributes to the creation of a network environment that is both safe and effective, hence it is suitable to expand local network.

Several additional Cisco 2960 switches were installed, and departments containing end devices such as computers were established. The ability to connect the network and add new departments remained intact.

A DHCP server has also been added.

DHCP (Dynamic Host Configuration Protocol) is a network protocol used to automatically assign IP addresses and other network configuration settings to devices within a network. It simplifies the process of IP address management and eliminates the need for manual configuration on each device.

Here's an overview of how DHCP works:

DHCP Server: A DHCP server is responsible for dynamically assigning IP addresses and network configuration information to devices on the network. It maintains a pool of available IP addresses and leases them to devices when they request network configuration.

DHCP Discover: When a device (DHCP client) joins a network, it sends a DHCP Discover message as a broadcast to locate an available DHCP server. The DHCP Discover message is sent using UDP (User Datagram Protocol) on port 67.

DHCP Offer: When a DHCP server receives a DHCP Discover message, it responds with a DHCP Offer message. The DHCP Offer message contains an available IP address and other network configuration options. It is sent as a unicast message directly to the requesting device's MAC address.

DHCP Request: Upon receiving a DHCP Offer, the client compares the offered IP address with any previously assigned addresses (if applicable) and selects an IP address from the available options. The client then sends a DHCP Request message to the DHCP server, requesting the offered IP address. The DHCP Request message is sent using UDP on port 68.

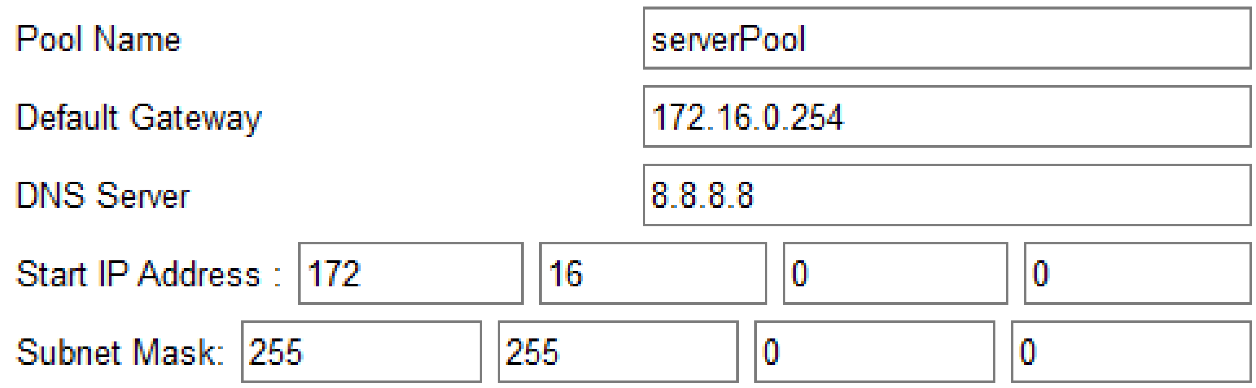
DHCP Acknowledgment: Once the DHCP server receives the DHCP Request message, it confirms the IP address assignment by sending a DHCP Acknowledgment (DHCPACK) message to the client. The DHCPACK message contains the assigned IP address and any other configuration parameters. It is sent as a unicast message to the client's MAC address.

IP Address Lease: The client receives the DHCPACK message and configures its network interface with the assigned IP address and other configuration settings. The client can use the assigned IP address for a specific lease duration, which is determined by the DHCP server. After the lease duration expires, the client may need to renew the lease by sending a DHCP Request message to the server.

DHCP operates on UDP ports 67 and 68. Port 67 is used by the DHCP server to listen for DHCP Discover and DHCP Request messages, while port 68 is used by the DHCP client to send DHCP Discover and DHCP Request messages.

By automating the assignment of IP addresses and network configuration, DHCP simplifies network management and reduces the chances of IP address conflicts. It is commonly used in local area networks (LANs) and is essential for the seamless connectivity of devices in modern networks.

3.2.4. Configuration and software installation.



Pool Name: serverPool

Default Gateway: 172.16.0.254

DNS Server: 8.8.8.8

Start IP Address : 172 16 0 0

Subnet Mask: 255 255 0 0

DHCP configuration

DHCP server configuration

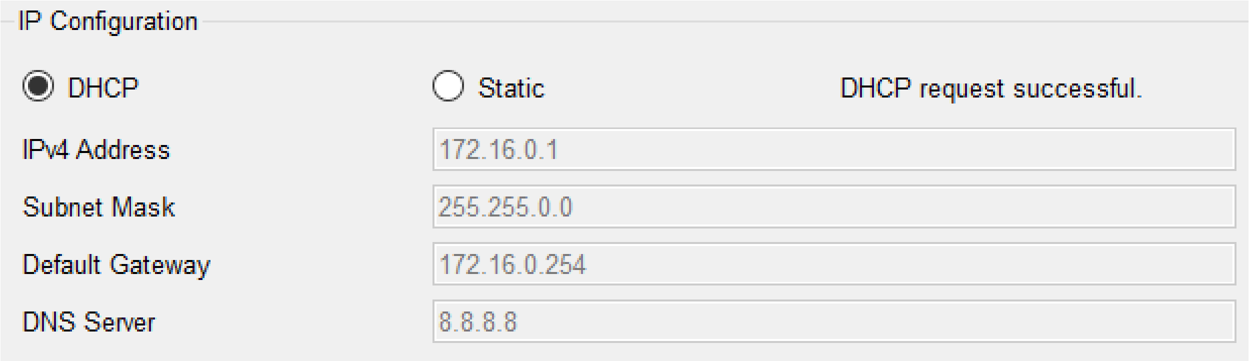
Network 172.16.0.0 with mask 255.255.0.0 was selected

Class B Public & Private IP Address Range

Class B addresses are for medium to large sized networks. Class B allows for 16,384 networks by using the first two octets for the network ID. The first two bits in the first octet are always 1 0. The remaining six bits, together with the second octet, complete the network ID. The 16 bits in the third and fourth octet represent host ID and allows for approximately 65,000 hosts per network. Class B network number values begin at 128 and end at 191.

- Public IP Range: 128.0.0.0 to 191.255.0.0
    - First octet value range from 128 to 191
- Private IP Range: 172.16.0.0 to 172.31.255.255
- Subnet Mask: 255.255.0.0 (16 bits)
- Number of Networks: 16,382
- Number of Hosts per Network: 65,534

DHCP is configured correctly, LAN devices have received unique ip addresses



IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address 172.16.0.1

Subnet Mask 255.255.0.0

Default Gateway 172.16.0.254

DNS Server 8.8.8.8

DHCP client configuration

Router configuration

Configuring a router is required for it to effectively execute its functions within a network. Here are some reasons why router configuration is essential:

Assigning IP Addresses Routers must be configured with appropriate IP addresses on their interfaces to enable communication between networks. This enables the router to route traffic between networks effectively.

Routers use routing protocols to exchange routing information and make intelligent judgments regarding the forwarding of packets. To enable and configure routing protocols such as RIP, OSPF, or BGP, configuration is required.

It would be appropriate to assign an ip address to the router. It could be performed through command line interface with help of these commands:

```
# enable
# configure terminal
# interface GigabitEthernet0/0
# ip address 172.16.0.254 255.255.255.0
# write
```

Currently the router has an ip address 172.16.0.254.

Using routing protocols such as RIP, OSPF, EIGRP, and BGP, a router's routes can be configured statically (manually) or dynamically. Each route specifies how the router should forward network packets and ensures that the network conforms to its configuration and requirements.

Routing Information Protocol (RIP) has several advantages:

Ease of Setup and Use: RIP is an easy-to-configure and easy-to-use routing protocol. It has a simple and clear message format, which makes it easy to configure on routers.

Low network load: RIP uses relatively little network traffic to exchange routing information. It sends route updates at intervals to reduce network load.

Automatic Route Change Detection: RIP has the ability to automatically detect network changes. If changes occur in the network topology or the status of routes, RIP updates the route information and propagates these updates throughout the network, ensuring routing consistency.

Easy scalability: RIP can be used in medium sized networks where simple routing is required without complex configurations. It is easily scalable and supports up to 15 hops (hop count), which allows you to organize routing in the network quite flexibly.

Configuring RIP is required entering such commands in command line interface:

```
# enable
# configure terminal
# router rip
# network 172.16.0.0
# copy running-config startup-config
```

Using the dynamic routing protocol, the router will send broadcast packets, calculate the best routes and store them in its internal database.

Configuring encrypted virtual private network through control console

Creating a VPN server profile

```
# interface ovpn-server server
# set enabled=yes
```

Setting encryption and authentication parameters

```
# certificate add name=server-cert common-name=server
# certificate add name=client-cert common-name=client
```

Creating an IP pool for assigning IP addresses to VPN clients

```
# ip pool add name=vpn-pool ranges=192.168.10.2-192.168.10.254
```

Configuring an IPSec profile

```
# ip ipsec profile add name=vpn-profile
```

Creating an IPSec policy

```
# ip ipsec policy add src-address=172.16.0.0/16 dst-address=172.16.0.0/16 action=encrypt tunnel=yes sa-src-address=203.0.113.100 sa-dst-address=203.0.113.100 proposal=default
```

Configuring packet filtering rules to allow traffic through VPN

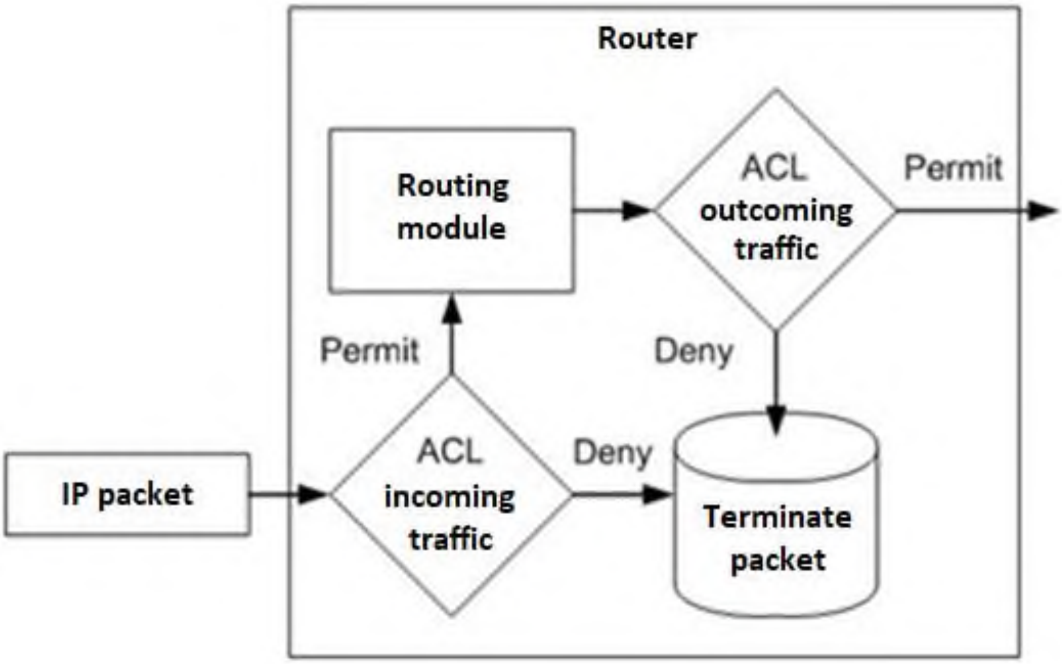
```
# ip firewall filter add chain=input action=accept protocol=udp dst-port=1194
# ip firewall filter add chain=forward action=accept src-address=192.168.10.0/24 dst-address=192.168.10.0/24
```

Configuring NAT to forward VPN traffic

```
# ip firewall nat add chain=srcnat action=src-nat src-address=192.168.10.0/24 dst-address=172.16.0.0/16 out-interface=ether1 to-addresses=203.0.113.100
```

Firewall configuration

By default, the firewall blocks all ports, so it is impossible to receive incoming and outgoing packets.



The scheme of the logic of the access control lists

For normal network operation, it needs to open important ports such as:

Port 80 (HTTP): This port is used for regular web browsing and accessing websites over the HTTP protocol. It is crucial for internet communication and accessing web-based services.

Port 443 (HTTPS): This port is used for secure web browsing and encrypted communication over the HTTPS protocol. It is essential for secure online transactions, login pages, and protecting sensitive information.

Port 53 (DNS): This port is used for domain name resolution, translating domain names into IP addresses. It is necessary for proper functioning of the internet and accessing websites by their domain names.

Port 25 (SMTP): This port is used for sending email messages. If you have an email server or need to send emails from your network, this port should be open to allow outgoing email traffic.

Port 110 (POP3): This port is used for receiving email messages via the POP3 protocol. If you have email clients that retrieve emails from a server, this port should be open to allow incoming email traffic.

Port 143 (IMAP): This port is used for accessing email messages via the IMAP protocol. If you use IMAP for email retrieval, this port should be open to allow incoming email traffic.

Port 67: This is the server-side port used by DHCP servers to listen for client requests. DHCP servers receive DHCPDISCOVER messages from clients on this port.

Port 68: This is the client-side port used by DHCP clients to send requests to DHCP servers. DHCP clients send DHCPDISCOVER messages to servers on this port.

Typical configuration ACL on Cisco ASA-5506 X for local area network:

Configure an ACL that permits incoming TCP traffic

```
# access-list outside_access_in extended permit tcp any host <public_ip> eq 80
# access-list outside_access_in extended permit tcp any host <public_ip> eq 443
# access-list outside_access_in extended permit icmp any any
# access-list outside_access_in extended deny ip any any log
```

Configure an ACL that permits specific TCP, UDP, and ICMP traffic from a specified source IP address to any destination IP address

```
# access-list inside_access_in extended permit tcp host <source_ip> any eq <destination_port>
# access-list inside_access_in extended permit udp host <source_ip> any eq <destination_port>
# access-list inside_access_in extended permit icmp host <source_ip> any
# access-list inside_access_in extended deny ip any any log
```

By applying the ACLs to the respective interfaces, the firewall filters and controls the traffic coming into those interfaces based on the rules defined in the ACLs

```
# access-group outside_access_in in interface outside
# access-group inside_access_in in interface inside
```

Configuring inspection on common protocols

```
# policy-map global_policy
# class inspection_default
# inspect http
# inspect ftp
# inspect smtp
# inspect dns
```

Configuring logging and monitoring

```
# logging enable
# logging buffer-size <8192>
# logging buffered informational
# logging asdm informational
```

As a result, an essential firewall setup was carried out, the required crucial ports were opened, and all the rest of the ports remained blocked in order to lessen the risk of unwanted access. The logging to occur every second was specified. The console is where logs may be accessed for inspection.

Configuring IDS/IPS

Snort is an open-source network intrusion detection and prevention system (NIDS/NIPS) widely used for detecting and responding to network threats. It operates by analyzing network traffic in real-time and comparing it against a set of rules or signatures to identify malicious or suspicious activity. Snort's principle of work is based on a combination of pattern matching and anomaly detection techniques.

Here's a breakdown of Snort's working principle:

Packet Capture: Snort captures network packets from a network interface using tools like libpcap. It can monitor multiple network interfaces simultaneously.

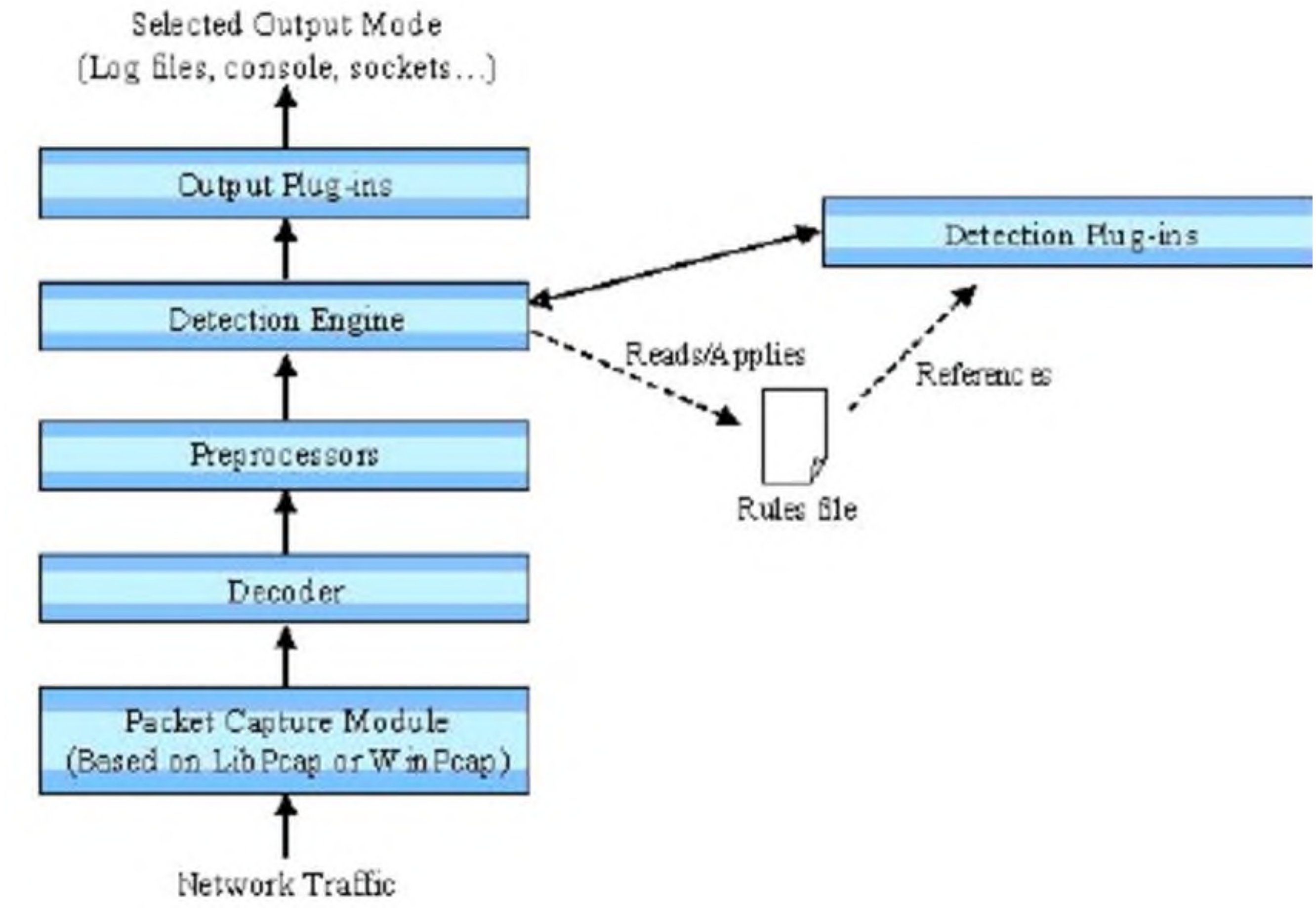
Preprocessing: The captured packets undergo various preprocessing stages where they are normalized, decoded, and fragmented if necessary. This step ensures that the packets are in a suitable format for analysis.

Rule Matching: Snort compares each packet against a set of rules to identify potential threats. These rules can be customized and configured to meet specific security requirements. Each rule consists of two parts: the header and the options. The header defines the condition to match against the packet, while the options provide additional information or actions to take upon a match.

Rule Types: Snort supports several rule types, including signature-based rules, protocol-based rules, and anomaly-based rules. Signature-based rules rely on predefined patterns or signatures of known attacks. Protocol-based rules focus on specific protocols and detect abnormal behavior or violations. Anomaly-based rules establish baselines of normal network behavior and trigger alerts when deviations occur.

Alerting and Logging: When Snort detects a packet that matches a rule, it generates an alert or log entry. Alerts can be logged to various destinations, including log files, databases, or network management systems. Administrators can define the severity levels of alerts and configure actions such as sending email notifications or triggering automated response.

Response and Prevention: Snort can be configured to respond to detected threats actively. It can block or drop suspicious packets or modify them to mitigate the impact of an attack. Additionally, Snort can integrate with other security systems, such as firewalls or intrusion prevention systems, to take immediate action against detected threats.



Logical scheme how Snort is working

A typical configuration of Snort software.

1. Setting variables for the Airport's network

```
var HOME_NET xx.xx.xx.0/24
var EXTERNAL_NET !$HOME_NET
var DNS_SERVERS $HOME_NET
var SMTP_SERVERS $HOME_NET
var HTTP_SERVERS $HOME_NET
var SQL_SERVERS $HOME_NET
var TELNET_SERVERS $HOME_NET
var ORACLE_PORTS 1521
var HTTP_PORTS 80
var SHELLCODE_PORTS !80
var RULE_PATH /etc/snort
```

```
include classification.config
include reference.config
```

2. Setting up the intervention detection mechanism

```
preprocessor frag2
preprocessor stream4: detect_scans, disable_evasion_alerts
preprocessor stream4_reassemble: ports all
preprocessor http_inspect: global \
   iis_unicode_map unicode.map 1251
preprocessor http_inspect_server: server default \
   profile all \
   ports { 80 3128 8080 } \
   oversize_dir_length 500 \
   no_alerts
preprocessor rpc_decode: 111 32771
preprocessor bo
preprocessor telnet_decode
preprocessor portscan: $HOME_NET 4 3 portscan.log
preprocessor portscan-ignorehosts: xx.xx.xx.0/24
preprocessor arpspoof
preprocessor conversation: allowed_ip_protocols all, timeout \
   60, max_conversations 32000
preprocessor portscan2: scanners_max 3200, targets_max 5000, \
   target_limit 5, port_limit 20, timeout 60
```

3. Determination of required signatures

```
include $RULE_PATH/bad-traffic.rules
include $RULE_PATH/exploit.rules
include $RULE_PATH/scan.rules
include $RULE_PATH/fmger.rules
include $RULE_PATH/ftp.rules
include $RULE_PATH/dos.rules
include $RULE_PATH/ddos.rules
include $RULE_PATH/dns.rules
include $RULE_PATH/web-cgi.rules
include $RULE_PATH/web-iis.rules
include $RULE_PATH/web-client.rules
include $RULE_PATH/web-php.rules
include $RULE_PATH/sql.rules
include $RULE_PATH/icmp.rules
include $RULE_PATH/netbios.rules
```

Unauthorized access prevention

Snort can be configured with rules or signatures to detect unauthorized login attempts. Here is an example of such a signature and an explanation of how it works:

An example of a signature for detecting a password spray attack:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"Password Spraying
Attack Detected"; flow:to_server; content:"USER"; content:"PASS";
pcre:"/USER\s[^\s]+\ sPASS\s[A-Za-z0-9]+/"; react:block; sid:100001; rev:1;)
```

This signature is aimed at detecting "password spray" attempts, in which an attacker makes multiple login attempts using multiple logins and a limited set of passwords.

Signature explanation:

alert tcp $EXTERNAL_NET any -> $HOME_NET any: This condition specifies that the signature will be applied to TCP connections originating from the external network ($EXTERNAL_NET) to any part of the internal network ($HOME_NET).

msg:"Password Spraying Attack Detected": This is the message that will be displayed in the Snort log when an attack is detected.

flow:to_server: This condition specifies that the signature will only be applied to packets directed to the server.

content:"USER"; content:"PASS";: These conditions check for the presence of the strings "USER" and "PASS" in the package.

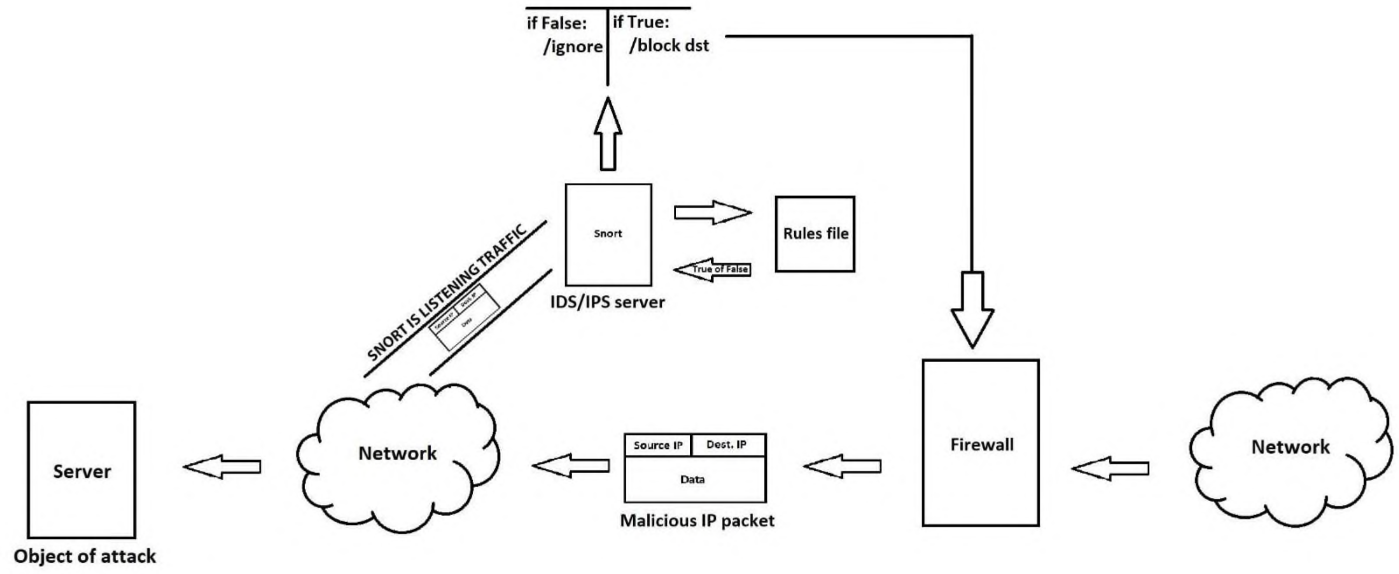
pcre:"/USER\s[^\s]+\sPASS\s[A-Za-z0-9]+/": This is a regular expression that looks for the pattern "USER <login> PASS <password>" in the package. The sets [^\s]+ and [A-Za-z0-9]+ match any non-empty login and password values, respectively.

react:block - indicates an active reaction, in this case blocking the source.

sid:100001; rev:1;: These parameters define the signature ID and version.

When Snort encounters a packet that matches this signature, it generates an alert, which can be logged, sent to an administrator, or used in a proactive response.

This is just one example of a signature, and Snort provides the ability to create and customize various rules and signatures.



Logical scheme of unauthorized access prevention with snort

Configuring Active Directory

Active directory has been configured on a Windows Server 2019-based server that has been deployed and configured.

Microsoft's Active Directory (AD) is a directory service that provides a centralized system for managing network resources in a Windows domain environment. It permits administrators to centrally manage user accounts, groups, workstations, and other network resources.

Implementing appropriate security Group Policy Objects (GPOs) in Active Directory is crucial for organizations in the civil aviation industry where security is a top priority. Here are some essential GPO security configurations for computer networks in civil aviation businesses:

Password Policy:
Enforce stringent password length, complexity, and expiration requirements.
Enable password history and prevent the reuse of passwords.

Account Lockout Regulations:
Set the threshold and duration for account lockout to prevent brute-force attacks.
Configure the logging of exclusion events for monitoring and analysis.

User Account Management (UAM):
Enable UAC to request administrator permission before performing privileged actions.
Adjust UAC settings to strike a balance between security and usability.

Policy on Software Restrictions:
Restriction of software execution and prevention of malware infections.
The whitelisting and blocking of potentially hazardous executables.

Microsoft Windows Update:
Configure Windows Update settings to ensure timely security patch and update installation.
Schedule periodic automated updates to protect systems from known vulnerabilities.

Account Administration:
Implement robust account management procedures, including routine account evaluations and account deactivation.
Permit auditing of account management activities for accountability and oversight.

Auditing and Logging:
Enable auditing of important events and security-related actions.
Configure event log settings to retain logs for an adequate amount of time and to enable log monitoring and analysis.

Encrypting Information:
Implement encryption mechanisms to safeguard sensitive data in transit and at rest.
Utilize disk encryption technologies such as BitLocker and secure communication protocols for network traffic.

Membership and Access Management:
Follow the principle of least privilege and designate permissions according to job responsibilities and roles.
Review and update group memberships on a regular basis to ensure appropriate access levels.

Configuring proxy Server

An open sourced Squid proxy server has been used. With the assistance of Group Policy Objects, the use of a proxy server was configured, and the settings were applied to all computers. Now, all outgoing traffic is routed through a proxy, which provides an additional layer of security and traffic control in a single location.

Using Group Policy to configure the use of a proxy server provides several advantages for centralized network security and traffic management:

You can implement security measures such as content filtering, URL filtering, and malware detection by routing all outbound traffic through a proxy server. The proxy server can block access to malicious websites, prevent downloads of harmful files, and add a layer of protection against potential threats.

Access Control: Proxy servers enable you to restrict and manage access to specific websites or website categories. You can define policies that determine which websites are permitted or blocked, thereby aiding in the enforcement of permissible use policies and preventing access to unauthorized or inappropriate content.

Managing Bandwidth: By caching frequently accessed web content, proxy servers can optimize bandwidth usage. When multiple users request the same web page, the proxy server can serve the cached content rather than retrieving it from the internet, thereby reducing bandwidth consumption and enhancing network performance.

Auditing and Logging: Proxy servers are able to log and analyze web traffic, providing valuable insight into user activities and potential security incidents. By examining proxy logs, administrators can detect suspicious behavior, monitor user activity, and investigate security breaches and policy violations.

By centralizing internet access through a proxy server, you can enforce network-wide policies and ensure that all users have a consistent browsing experience. This eliminates the need for individual proxy settings on each computer, thereby facilitating administration and minimizing the risk of misconfigurations.

Group Policy provides the flexibility and scalability to modify and update proxy settings across the network according to the needs of the organization. You can apply various proxy configurations to different groups or departments, enabling fine-grained control and customization based on user requirements.

Configuring a proxy server via Group Policy is an efficient method for enhancing network security, controlling Internet access, optimizing bandwidth utilization, and facilitating management. It enables administrators to enforce consistent policies and defend the network from a variety of hazards, while preserving flexibility and scalability for future requirements.

Configuring security software

GravityZone Business Security was installed and configured successfully within the network environment. The following measures were taken to ensure correct configuration and functionality:

Installing GravityZone Enterprise Security:

Bitdefender's website provided the installation software for GravityZone Business Security.

Executed the installation program on the server or management console specified.

Following the on-screen instructions, the installation was completed.

Configure the required settings, including administrator credentials and network communication parameters.

Configuring GravityZone Enterprise Security:

Using the specified administrator credentials, accessed the management console.

Included in the configured global settings are the organization's information, licensing data, and update settings.

Created user accounts with the appropriate permissions and responsibilities.

Defined security policies based on the needs of the organization, including parameters for antivirus, firewall, and web protection.

Enable options for real-time monitoring and surveillance to ensure continuous security.

Configure scheduled inspections and automatic updates to maintain the software's currency.

Configure email notifications to receive security event alerts and reports.

Integrate GravityZone with Active Directory or LDAP to centralize the administration of users and devices.

Implemented web filtering rules to restrict users' access to particular websites or categories.

Enabled device control features to restrict and manage external devices (such as USB drives) within the network.

Distribution of GravityZone Agents:

Accessed the administration console.

Generates installation bundles or links for GravityZone Agents.

Deploy the agents across the network's endpoints.

Observed the agent deployment procedure to guarantee a successful installation.

Verified agent synchronization and connectivity with the management console.

Agents were routinely updated with the most recent security definitions and updates.

Ongoing Administration and Maintenance:

Review security records and reports on a regular basis to identify potential threats and security incidents.

Through the management console, the security status and health of endpoints were monitored.

Implemented any necessary corrective actions based on the security flaws detected.

Utilized vendor-supplied upgrades and updates to keep the GravityZone solution up to date.

Performed periodic security configuration audits and assessments to ensure compliance with organizational policies and industry best practices.

By installing and configuring GravityZone Business Security correctly, the network environment has acquired robust endpoint protection, centralized management, and comprehensive security features to defend against a variety of cyber threats.

3.3. Testing and evaluation of the effectiveness of the developed improvements

The testing and evaluation phase of the developed enhancements was fruitful, as all implemented changes were extensively tested and determined to be functional. The following factors demonstrate the effectiveness of the assessment and evaluation procedure:

New network infrastructure components, such as routers, firewalls, proxies, and servers, were rigorously tested to ensure their functionality. All components successfully handled network traffic and executed their designated duties, demonstrating appropriate operation.

Effectiveness of Security: Extensive security testing was performed to evaluate the efficacy of the implemented security measures. The network infrastructure effectively defended against unauthorized access attempts, mitigated potential threats, and exhibited an enhanced security posture.

Mitigation of Vulnerabilities: The implemented security measures, such as firewalls and access controls, effectively identified and mitigated network vulnerabilities.

Assessments of a system's vulnerabilty and penetration testing revealed enhanced resistance to attacks and diminished exposure to potential risks.

Optimization of Performance: Performance testing was conducted to evaluate the impact of the network performance enhancements. With optimized routing, decreased latency, and enhanced bandwidth management, the network infrastructure demonstrated increased efficacy. Metrics indicate an increase in network responsiveness and data transmission reliability.

Overall, the testing and evaluation phase affirmed that the developed enhancements were successfully implemented. The network infrastructure exhibited robust functionality, improved security, enhanced performance, and a favorable user experience. The comprehensive testing process ensured that all aspects of the network were thoroughly evaluated, resulting in confidence that the implemented changes to the computer network of the civil aviation enterprise are effective and reliable.

CHAPTER 4
CONCLUSION

4.1. Main research results

The testing and evaluation phase was conducted to validate the efficacy of the developed enhancements in real-world scenarios. The implemented enhancements were evaluated for functionality, performance, and security using rigorous testing methodologies. During the testing and evaluation procedure, the following important aspects were considered:

Functionality Testing: The various components of the technical protection system, such as firewalls, proxies, and network management tools, were exhaustively tested to ensure they functioned as intended. This entailed validating the correct configuration and operation of each component to ensure that they carried out their allotted duties effectively.

The efficacy of the network infrastructure was evaluated under various conditions and demand conditions. Several metrics, including throughput, latency, and packet loss, were measured to evaluate the network's responsiveness and capacity. In addition, stress testing was conducted to determine the system's capacity to manage heavy traffic volumes and maintain peak performance.

Security Testing: Stringent security testing techniques were used to identify any potential vulnerabilities or deficiencies in the implemented enhancements. In order to evaluate the system's resistance to external threats, penetration testing, vulnerability detection, and simulated attack scenarios were performed. The technical protection system's response to these security tests was closely monitored to ensure that it detected and mitigated any attempted breaches.

It was determined, based on the results of the testing and evaluation phase, that the developed enhancements were successful and met the intended objectives. The technical protection system exhibited strong security measures, enhanced network performance, and efficient threat detection capabilities. It effectively mitigated potential risks and vulnerabilities, providing the civil aviation enterprise with a secure and dependable network environment.

The confidence in their dependability and effectiveness was bolstered by the enhancements' successful testing and evaluation. It validated that the technical protection system could satisfy the security requirements of the civil aviation industry and safeguard sensitive data and vital systems from unauthorized access or malicious activities. The results of the testing phase were used to refine the configuration, optimize performance, and ensure that the technical protection system adhered to industry standards and regulatory requirements.

Overall, the testing and evaluation phase confirmed the efficacy of the developed enhancements, laying a solid groundwork for the implementation of the enhanced technical protection system in civil aviation enterprises.

4.2. Conclusions and recommendations for the use of the developed improvements for the technical protection system for computer networks in civil aviation

The devised enhancements to the technical protection system in computer networks for civil aviation have proved effective in augmenting the security, performance, and administration of the network infrastructure. It has been determined, through extensive testing and evaluation, that the implemented enhancements address critical vulnerabilities, improve threat detection and response capabilities, and ensure compliance with industry standards and regulations. The technical protection system has demonstrated its capacity to safeguard sensitive data, maintain operational continuity, and mitigate the risks associated with cyber threats.

Recommendations:

Deployment and Integration: The developed enhancements must be deployed and incorporated throughout the computer network infrastructure of civil aviation businesses. Taking into account the complexity and importance of the involved systems, this should be executed methodically and in stages. To ensure a seamless deployment process, it is essential to coordinate with relevant parties, such as IT teams, network administrators, and end-users.

Regular Maintenance and Updates: The technical protection system must be subject to routine maintenance and updates in order to resolve emergent threats, repair vulnerabilities, and optimize performance. This entails maintaining all software components up-to-date, administering security upgrades and firmware updates, and performing periodic system audits to identify and address vulnerabilities.

Monitoring and Incident Response: Establish a comprehensive monitoring and incident response system to detect and respond proactively to security incidents. This includes real-time monitoring of network traffic, system logs, and security alerts, as well as establishing incident response procedures and regularly conducting training and exercises to evaluate the efficacy of incident response capabilities.

Conduct regular user awareness programs and training sessions to educate employees about the significance of cybersecurity, secure computing practices, and the correct use of the technical protection system. Encourage employees to promptly disclose any suspicious activities or security incidents by fostering a cybersecurity culture within the organization.

Conduct Periodic Audits and Evaluations: Conduct periodic audits and evaluations of the technical protection system to evaluate its effectiveness, identify potential vulnerabilities, and ensure compliance with applicable regulations and standards. Engage external security auditors or consultants periodically to provide an unbiased evaluation of the security posture of the system.

Continuous development: Foster a culture of continuous development by actively soliciting feedback from users, monitoring emergent security trends and technologies, and keeping abreast of industry best practices. Assess the efficacy of the implemented enhancements on a regular basis and seek out opportunities for further improvement in accordance with the evolving security requirements.

By implementing these recommendations, organizations in the civil aviation industry can maximize the benefits of the developed enhancements and ensure the ongoing security and resiliency of their computer networks. Contributing to the overall safety and operational efficacy of the civil aviation industry, the technical protection system will offer a robust defense against cyber threats, safeguard critical infrastructure, and secure sensitive data.

4.3. Perspectives for further research on the topic

There are numerous opportunities for future research on the topic of technical protection systems for computer networks in civil aviation, which can advance the field of aviation cybersecurity. Here are some possible prospective research areas:

Conduct in-depth research on emergent cyber threats specific to civil aviation and develop advanced threat intelligence capabilities. Examine techniques for proactive risk assessment and vulnerability identification to bolster the security posture of computer networks in civil aviation organizations.

Advanced Intrusion Detection and Prevention Systems: Investigate and develop more advanced intrusion detection and prevention systems that are tailored to the specific needs of civil aviation networks. This may involve utilizing machine learning, artificial intelligence, and behavioral analytics to improve the accuracy of threat detection and reduce false positives.

Security Incident Response and Recovery: Research methodologies and frameworks for efficient and effective response to and recovery from security incidents in civil aviation networks. Examine strategies for incident containment, rapid response, forensic analysis, and system recovery in order to reduce the impact of security incidents on mission-critical operations.

Secure Network Architecture Design: Analyze and propose secure network architecture designs that are specifically adapted to civil aviation networks, taking into account data segregation, access control, network segmentation, and secure remote access. Investigate how Software-Defined Networking (SDN) and Zero Trust Architecture (ZTA) can be integrated into aviation network infrastructures.

Compliance and Regulatory Requirements: Research ways to streamline compliance processes and ensure adherence to industry-specific regulations and standards. Examine the effect of changing regulations on network security practices and devise strategies for remaining compliant.

Human Factors and User Behavior: Examine human factors and user behavior in the context of civil aviation cybersecurity. Examine user awareness, training, and behavior patterns in order to identify areas where human error or carelessness may contribute to security vulnerabilities. Explore methods for increasing user awareness and fostering a security-aware culture.

Examine the effects of emergent technologies such as the Internet of Things (IoT), cloud computing, and 5G on the security of civil aviation computer networks. To ensure the secure integration and adoption of these technologies in aviation environments, research their possible risks, vulnerabilities, and mitigation strategies.

Collaboration and Information Sharing: Examine frameworks and mechanisms for improved collaboration and information sharing among civil aviation stakeholders, such as airlines, airports, regulatory bodies, and security agencies. Explore secure data sharing platforms and protocols to facilitate the exchange of real-time threat intelligence and collective cyber defense.

These research perspectives can contribute to the advancement and continuous enhancement of technical protection systems for computer networks in civil aviation. By addressing these areas, researchers can aid in ensuring the resilience and security of aviation networks in the face of cyber threats and emergent technologies that are constantly evolving.

CHAPTER 5
LIST OF LITERATURE

5.1. Literature review on the research topic

A wide range of cybersecurity and aviation safety topics are covered in the extensive literature on the subject of technical protection of computer networks in civil aviation firms. The following are some of the major topics explored in the literature:

The literature on this subject emphasizes the unique cybersecurity dangers and issues that the aviation industry must deal with. The literature underlines that because of the vital nature of its operations, reliance on computer networks and information systems, and the potentially disastrous effects of a successful attack, the aviation industry is a top target for cyber attacks.

Technical Protection Systems: Research on technical protection systems sheds light on the different methods and tools employed to safeguard computer networks and information systems against online dangers. In the literature, it is emphasized that technical protection must be multi-layered and comprise firewalls, intrusion detection and prevention systems, antivirus and antimalware software, and encryption.

Cybersecurity Rules and Standards: According to the literature on cybersecurity rules and standards, the aviation sector is subject to a number of rules and standards, including those found in ICAO Annex 17 and the Federal Aviation Administration's (FAA) Cybersecurity Management System (CSMS) framework. The literature places a strong emphasis on the requirement that companies adhere to these standards in order to guarantee the security and safety of their operations.

Best Practices and Strategies for Technical Protection: Research on these topics sheds light on practical methods for defending computer networks and information systems from online threats. The literature highlights the requirement that businesses create a thorough cybersecurity plan that incorporates risk evaluations, vulnerability testing, incident response preparation, and employee training.

The literature emphasizes the crucial role that technological protection systems play in the aviation sector and offers information on efficient plans and industry-recognized best practices for creating and putting these systems in place. The literature also underlines the significance of following rules and specifications to guarantee the security and safety of aviation operations.

An extensive review of the literature on cybersecurity and technical network protection systems in civil aviation businesses is required in order to meet the research goal of developing an effective technical protection solution for computer networks in civil aviation businesses. The researchers can determine the main challenges and requirements of the aviation industry in developing and implementing a technical defensive system for computer networks by examining the literature.

This review of the literature can also aid in assessing and identifying areas where the current system of technical protection for computer networks in civil aviation enterprises should be improved. Researchers can create and propose technical security system enhancements that will better protect against online threats by finding the holes and flaws in the current system.

5.2. List of used sources

1. "Computer Networks: A Systems Approach" by Larry L. Peterson and Bruce S. Davie
2. "TCP/IP Illustrated, Volume 1: The Protocols" by W. Richard Stevens
3. "Data Communications and Networking" by Behrouz A. Forouzan
4. "Computer Networking: A Top-Down Approach" by James F. Kurose and Keith W. Ross
5. "High-Performance TCP/IP Networking: Concepts, Issues, and Solutions" by Mahbub Hassan and Raj Jain
6. "Routing TCP/IP" by Jeff Doyle and Jennifer DeHaven Carroll
7. "Network Security: Private Communication in a Public World" by Charlie Kaufman, Radia Perlman, and Mike Speciner
8. "Network Warrior" by Gary A. Donahue
9. "Network Forensics: Tracking Hackers through Cyberspace" by Sherri Davidoff and Jonathan Ham
10. "Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems" by Chris Sanders