MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
NATIONAL AVIATION UNIVERSITY

Air Transportation Management Department

PERMISSION TO DEFEND GRANTED
Head of the Department
_____Yun G.M.
“_____”_____2020

MASTER THESIS
(EXPLANATORY NOTES)

Theme: “Methods and tools to ensure information security in aviation enterprises”

Done by: Mariana Ye. Khodurska

Supervisor: Victoria Yu. Ivannikova, PhD, Associate professor

Advisers on Individual Parts of the Notes:

Theoretical Part - Victoria Yu. Ivannikova , PhD, Associate professor

Analytical Part – Victoria Yu. Ivannikova, PhD, Associate professor

Design Part – Victoria Yu. Ivannikova, PhD, Associate professor

Standards Inspector: Yulia V. Shevchenko PhD, Associated professor

Kyiv 2020

Міністерство освіти і науки україни
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Кафедра організації авіаційних перевезень

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____Юн Г.М.
«_____»_____2020 р.

ДИПЛОМНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
«МАГІСТР»

Тема: «Методи забезпечення інформаційної безпеки авіапідприємств»

Виконавець: Ходурська Мар’яна Єгорівна

Керівник: к.т.н., доцент кафедри організації авіаційних перевезень НАУ Іваннікова Вікторія Юріївна

Консультанти з окремих розділів пояснювальної записки:

Теоретична частина – к.т.н., доцент, Іваннікова Вікторія Юріївна

Аналітична частина – к.т.н., доцент, Іваннікова Вікторія Юріївна

Проектна частина – к.т.н., доцент, Іваннікова Вікторія Юріївна

Нормоконтролер: к.е.н., доцент, Шевченко Юлія Вікторівна

Київ 2020

NATIONAL AVIATION UNIVERSITY

Faculty of Transport, Management and Logistics

Air Transportation Management Department

Specialty: 275 “Transport Technolgies”

Educational-Professional Program: Air Transportation Management

APPROVED BY
Head of the Department
_____Yun G.M
“__–___” ____2020

TASK

of completion the master thesis

Mariana Ye. Khodurska

1. Theme of the master thesis entitled “Methods and tools to ensure information security in aviation enterprises” was approved by a decree of the Rector order № 2401/st. of October 17th, 2019.
2. Term performance of thesis: from October 14th to December 29th, 2019 and from January 20th to February 9th of year 2020 .
3. Initial data required for writing the master thesis: statistics of the State Statistics Committee of Ukraine, State Aviation Administration, SITA analytics and data, reports of “UIA” by using the method of financial and economic analysis, statistical analysis and investment analysis, ISO 27001 and ISO 27002.
4. Content of the explanatory notes: introduction, theoretical part, analytical part, design part, conclusions and appendices.
5. List of mandatory graphic materials: Critical Infrastructure Sectors, USAP audit assistance, Amount of passengers by months in 2013-2019, Growth of passenger traffic in 2013 – 2019, Number of flights performed by UIA in 2013-2019, Amount of cargo and mail transportation in 2013 – 2019, Financial indocators of UIA 2013-2018, SWOT analysis of UIA, The percentage of IT budget spent on Cybersecurity, The percentage of organizations with a formal Information Security Strategy.

6. Planning calendar

№	Assignment	Deadline for completion	Mark on completion
1.	Gather information regarding information and cyber security in aviation industry	14.10.19 – 27.10.19	done
2.	Collect and process statistical data and analyze Ukrainian aviation industry. Review the activity of Ukraine International Airlines	28.10.19 – 05.11.19	done
3.	Gather the information security statistical data	05.11.19 – 15.11.19	done
4.	Compare information security regulations and experiences of other countries	16.11.19 – 28.11.19	done
5.	Investigate and propose the procedure of information security audit	29.11.19 – 16.12.19	done
6.	Suggest an idea of internal audit calculation	17.12.19 – 09.02.19	done

7. Advisers on Individual Parts

Part	Advisor (position, name)	Date, signature	
		Task given	Task received
Theoreticalpart	Ivannikova V.Yu.	14.10.2019	27.10.2019
Analytical part	Ivannikova V.Yu.	28.10.2019	28.11.2019
Design part	Ivannikova V.Yu.	29.11.2019	09.02.2020

8. Given date of the task: October 14, 2019

Supervisor of the bachelor thesis: Ivannikova V.Yu.

(signature) (name, surname)

The task was accepted for completion: Mariana Y. Khodurska

(signature) (name, surname)

REPORT

Explanatory note to the master thesis project “Methods and tools to ensure information security in aviation enterprises” consists of 135 pages, 39 figures, 17 tables, 44 sources used.

KEY WORDS: INFORMATION SECURITY, CYBER SECURITY, CYBERATTACK, INFORMATION SYSTEMS, AUDIT, PROCEDURE, INVESTIGATION, REGULATIONS.

Object of the master paper is information security and cyber security in aviation industry and air transportation enterprises. The thesis investigates Uktrainian International Airlines as an example of an air transportation enterprise.

Subjects of master paper are theoretical and practical aspects of implementing external and internal audit of information security for an air transportation enterprises.

Aim of the master paper is to define of information and cyber security threats and reasons for critical infrastructures and air transportation, investigate the information security audit procedure, its main parts and peculiarities, recommendation of information system audit procedure, examination of external and internal audits, propose the way to calculate audit costs and the audit duration.

While composing master thesis Ukrainian aviation industry and its’ business activity were investigated. Ukraine International Airlines were taken as an example of an aviation enterprise, because of being a major player on the aviation market in Ukraine. Also, there has been a focus on analizing appropriate ISO/IEC and Ukrainian regulations regarding information security audits.

The thesis is recommended to be used in future researche, educational process and for the practical implementation of the proposed improvements by Ukrainian airlines and other air transportation companies.

CONTENTS

LIST OF CONVENTIONAL SIGNS, ABBREVIATIONS AND TERMS

CAIS – critical aviation information system

ICAO – International Civil Aviation Organization

CA – civil aviation

EASA – European Aviation Safery Agency

ENISA – European Network and Information Security Agency

ECCSA – European Centre for Cyber Security in Aviation

USAP - Universal Security Audit Programme

SARPs – Standard and Recommended Practices

ISM – Information Security Management

ISMS – Information Security Management Systems

ISO – International Organization for Standartization

EPCIP – European Programme for Critical Infrastructure Protection

GCI – Global Cybersecurity Index

ESCP – European Strategic Coordination Platform

CISO – Chief Information Security Officer

PDCA - Plan - Do - Check - Act Method

INTRODUCTION

Air Transportation Management Department				*NAU 20.08.35.001EN*			
Researcher	*Mariana Y. Khodurska*			*INTRODUCTION*	*Letter*	*Sheet*	*Sheets*
Supervisor	*Ivannikova V.Yu*				*D*	*9*	*4*
Standards Inspector	*Yulia V. Shevchenko*				*FTML 275 ОП-202Ма*		
Head of the Department	*Yun G.M.*						

Relevance of the topic. The research topic is relevant due to the need to introduce a safety audit in the practice of Ukrainian enterprises. Emerging Information Technology is making a dramatic change in our lives. Information has become a commodity that can be bought, sold, exchanged. However, the cost of information is often many times greater than the cost of the computer system in which it is stored.

The degree of information security currently depends on the well-being and sometimes life of many people. To obtain objective qualitative and quantitative assessments of the current state of information security of the company, as well as recommendations on information risks, a systematic audit process of information security is conducted.

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) form a specialized system of worldwide standardization. At present, the international community has performed significant work towards standardizing information security management (ISMS) systems and individual IS management processes. The basis of such standardization was the ISO 9000 series of standards, which imposes requirements on quality management systems, the observance of which allows to control the quality of own products or services provided. Much has been taken of the ISO 9000 standards when developing standards for complex information security system, for example the basic approach is the process and use of the PDCA model for continuous improvement, both system and its individual processes.

Information Security audit is usually used to objectively assess the level of security of information systems (IS).

Information systems are widely implemented and used to process, store and transmit information. This, in turn, has led to the need to protect information systems, as information attacks can cause great financial and material losses. The aim of the audit is to develop effective measures to provide information security in companies, organizations and institutions.

The information security audit collects and analyzes the information regarding the information system under review. It is conducted with a view to quantitative as well as qualitative assessment of the level of protection of information system against possible

attacks. Today, it is advisable to carry out an audit of information security in various cases. The audit can be conducted both before the implementation of the security system and after the completion of this procedure. The audit also allows the previously established security system to be aligned with the updated requirements, to streamline and systematize existing measures aimed at ensuring information system protection.

It is the audit itself that can provide an objective assessment of the security of any type of enterprise or institution, as well as prevent the realization of potential threats. The result of the audit is the basis for further development of the information security. Also, keep in mind that auditing is not a one-off event, it should be done regularly. Only in this way will it be possible to realistically help to increase the level of information system protection.

The Information Security Incident Management System (ISIMS) is a basic component of the overall ISMS and allows to identify, account for, respond to and analyze information security events and incidents. Without implementing these processes, it is impossible to provide a level of security that is adequate to current industry standards. For the most effective implementation of the ISMS, it is necessary to rely on the requirements of international and industry standards, such as ISO \ IEC 27001: 2013 «Information security management systems. Requirements» and also ISO/IEC 27035:2011 «Information technology. Security techniques. Information security incident management».

The modern information system of the organization is a distributed and heterogeneous system that uses different software and hardware components and has access points in the public network (e.g. the Internet). In this regard, the task of correctly and securely configuring components and securing intereaction between components is significantly complicated, and as a result, the number of vulnerabilities in the system increases.

The presence of vulnerabilities in the system allows the potential intruder to carry out a successful attack and harm the activities of the organization. The occurrence of "weaknesses" may be due to various reasons, both objective (for example, deficiencies

in the underlying software) and subjective (for example, incorrect adjustment of the equipment).

Detecting and eliminating vulnerabilities, as well as assessing the overall security level, are an extremely important components of security, which can significantly increase the security level of information and other system resources.

Object of study. Information security and cyber security in aviation indystry and air transportation enterprices. The thesis investigates Uktrainian International Airlines as an example of an air transportation enterprise.

Subject of study are theoretical and practical aspects of implementing external and internal audit of information security for an air transportation enterprices.

The practical significance of the results. Theoretical and practical developments in the field of security audit, which are effectively used in the context of market relations, combined with the legal and socio-technological features of Ukraine, open up new opportunities to find a more sophisticated model of building an enterprise security audit. Under market conditions, not every management system will provide a 100% survival guarantee, but the enterprises, that have implemented a modern security audit system have better performance than enterprises operating on the basis of old management principles. In many developed countries, managers rely on the services of a dedicated security service. This objectively leads to a scientific and practical interest in research on enterprise security audits.

1. THEORETICAL PART

Air Transportation Management Department				*NAU 20.08.35.100 EN*			
Researcher	*Mariana Y. Khodurska*			*THEORETICAL PART*	*Letter*	*Sheet*	*Sheets*
Supervisor	*Ivannikova V.Yu*				*D*	*13*	*40*
Standards Inspector	*Yulia V. Shevchenko*				*FTML 275 ОП-202Ма*		
Head of the Department	*Yun G.M.*						

1.1. Concept of information security

Information systems and technology are closely associated with the aviation industry – development of technical documentation, production planning, and management of organization. An exchange of information both within the organization and beyond is constant. The problem of information security in aviation industry enterprises becomes more important every year.

With the increasing significance of information technology, there is an urgent need for adequate measures of information security. Systematic information security management is one of most important initiatives for IT management. At least since reports about privacy and security breaches, fraudulent accounting practices, and attacks on IT systems appeared in public, organizations have recognized their responsibilities to safeguard physical and information assets. Security standards can be used as guideline or framework to develop and maintain an adequate information security management system (ISMS) [1].

1.1.1. ISO standards regarding information security

The responsibility of the ISO is development and publishing of a broad spectre of international standards in various business and process areas. Some of these standards are very wide, while others are detailed and precise. The broad ISO standards are important because they allow all worldwide enterprices to be talking in the same language. ISO standards are much more specific and controlled than the Information Technology Infransructure Library (ITIL). The standards are published and controlled by the ISO organization in Geneva following strict copyright rules [2].

The standards ISO/IEC 27000, 27001 and 27002 are international standards that are receiving growing recognition and adoption. They are referred to as “common language of organizations around the world” for information security [3]. Figure 1.1 represent the structure of ISO 27000 family.

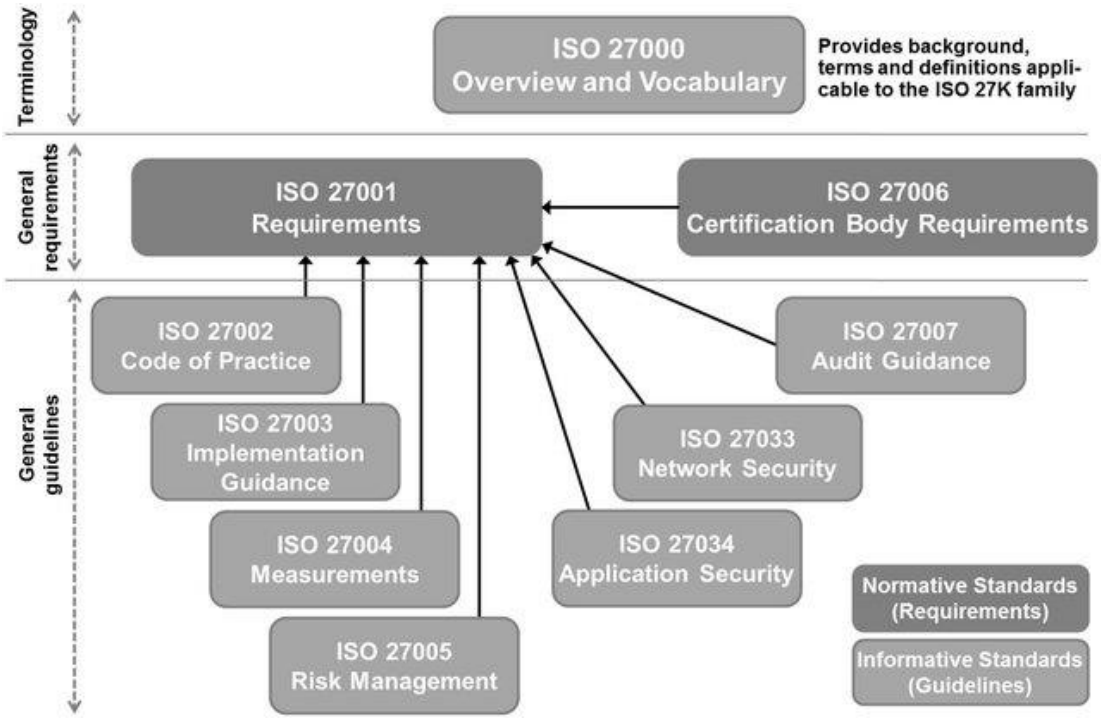

Fig.1.1. Structure of ISO 27000 family

There are two ISMS standards, ISO 27001 and ISO 27002. ISO 27001 states information security management standard on the control of documents for an ISMS. With ISO/IEC 27001 companies can have their ISMS certified by a third-party organization and thus show their customers evidence of their security measures. ISO 27002 represents an important IT-related security standard designed to help any enterprise that needs to establish a comprehensive information security management program or improve its current information security practices.

According to ISO 27002:2005, information is an asset which, like other important business assets, has a value to an organization and consequently needs to be suitably protected [5]. This is especially important in the increasingly interconnected business environment. As a result of this growing interconnectivity, data is increasingly exposed to a wider range of threats and vulnerabilities.

The ISO IEC 27002 is a standard concerning both a wide range of information sources and information security in a general sense [2]. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Whatever form

the information takes, or means by which it is shared or stored, it should always be appropriately protected [4]. Since information can exist in many forms, the ISO 27002 standard takes a very broad approach. It includes at least the following:

- Electronic files: software files, data and image files;
- Paper documents: printed materials, hand written notes, photographs and drawings;
- Recordings: video and audio
- Communications: telephone, mobile phone and face to face conversations; email, fax, video messages.

However, the term *information* includes not just words, numbers, and images, it also includes all kinds of ideas, concepts, and knowledge.

Information Security is information protecting practice that is implemented by mitigating the risks, that might occur in a certain industry. Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information, but not only securing information from unauthorized access.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes [4].

1.1.2. Information security history

Objectively, the category "information security" has risen with the advent of information communications between people, as well as with the awarenessof the presence in people and their communities of interests, which can be harmed by acting on the information communications, the presence and development of which provides and sets information exchange between all elements of society.

Given the impact on the transformation of information security ideas, in the development of information communications can be divided into several stages [5].

Stage I (before 1816) - is characterized by the use of naturally formed means of information communication. During this period, the main task of information security was to protect information about events, facts, property, location and other data of vital importance to the person or the community to which it belonged.

Stage II (from 1816) - is associated with the beginning of the use of artificially created technical means of telecommunication and radio. To ensure the secrecy and noise immunity of the radio, it was necessary to use the experience of the first period of information security at the highest technological level, namely the use of noise-proof encoding of the message (signal) with the subsequent decoding of the received message (signal).

Stage III (from 1935) - is associated with the advent of radar and sonar. The main way to ensure information security during this period was to use a combination of organizational and technical measures aimed at increasing the security of radar equipment against the action on their receiving properties.

Stage IV (from 1946) - is connected with the invention and implementation in practice of computers. Information security tasks were solved mainly by methods of limiting physical access to the equipment.

Stage V (from 1965) - is conditioned by creation and development of local information and communication networks. Information security tasks were also solved, mainly, by methods of physical protection and by administering and managing access to network resources.

Stage VI (from 1973) - involves the use of mobile communication devices with a wide range of tasks. Information security threats have become much more serious. New security criteria had to be developed to ensure information security in computer systems with wireless data networks. Communities of hackers have emerged, aiming at damaging the information security of individual users, organizations, and entire countries. The information resource has become the most important resource of the state

and its security is the most important and obligatory component of national security. Information law is emerging - a new branch of the international legal system.

Stage VII (from 1985) - is related to the creation and development of global information and communication networks using space security. It can be assumed that the next stage in the development of information security will obviously be related to the widespread use of communication devices with a wide range of tasks and global coverage in space and time provided by space information and communication systems. To solve the problems of information security at this stage, it is necessary to create a macrosystem of information security discussed by leading international forums.

In light of the development of new IT technologies, the concept of information security has expanded considerably. Some experts point out that it is more appropriate to completely replace the concept of information security with the concept of cybersecurity. This is due to the fact that much more than just the loss of information depends on the protection of processes, information and activity in cyberspace today. That is, the loss of information entails a number of other complex complications. Cybersecurity is protection against viruses, hacking and data tampering. Viruses, for example, can not only delete or steal data, but also affect employees' performance and productivity, or even halt production. Information can also be used against a person or structure.

On August 29, 2019, at the World Conference on Artificial Intelligence in Shanghai, Jack Ma and Ilon Musk discussed all the excitement of the public in recent years: “We are already cyborgs. People are so integrated with their phone and computer that they don't even realize it. When we forget mobile somewhere, it seems as if we have lost some of our body.” And so, it is. We are already fully connected to our phones, without which we cannot go anywhere and do not think life without them. Our phone is food, travel, maps, weather, sleep, health, and this list can be complemented by the many opportunities we live with every day [6].

1.1.3. Fundamental principles on information security

Information and the supporting processes, systems and networks are important business assets. Defining, achieving, maintaining, and improving information security may be essential to maintain competitive edge, cash flow, profitability, legal compliance, and commercial image.

Organizations and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Causes of damage such as malicious code, computer hacking, and denial of service attacks have become more common, more ambitious and increasingly sophisticated.

Information security is important to both public and private sector businesses and to protect critical infrastructures. In both sectors, information security will function as an enabler, e.g. to achieve egovernment or e-business, and to avoid or reduce relevant risks. The interconnection of public and private networks and the sharing of information resources increase the difficulty of achieving access control. The trend to distributed computing has also weakened the effectiveness of central, specialist control [7].

Many information systems have not been designed to be secure. The security that can be achieved through technical means is limited, and should be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail. Information security management requires, as a minimum, participation by all employees in the organization. It may also require participation from shareholders, suppliers, third parties, customers or other external parties. Specialist advice from outside organizations may also be needed.

Information Security programs are build around 3 objectives, commonly known as CIA triangle (Figure 2) – Confidentiality, Integrity, Availability.

Fig.1.2. The CIA triangle

Confidentiality – means information is not disclosed to unauthorized individuals, entities and process. For example, if we say I have a password for my Gmail account but someone saw while I was doing a login into Gmail account. In that case my password has been compromised and Confidentiality has been breached. Examples of confidentiality measureas are:

- Access to information is granted on a need to know basis. It is not necessary, for example, for a payroll employee to be able to see reports of discussions with the customer;
- Employees take measures ensuring that information does not find its way to those people who do not need it. They ensure, for example, that no confidential documents are lying on their desk while they are away (clear desk policy);
- Logical access management ensures that unathoprized persons or processes do not have access to automated systems, databases and programs. A user, for example does not have the right to change the settings of the PC;
- A separation of duties is created between the system development organization, the processing organization and the user organization. A system developer cannot, for example, make any changes to salaries;

- Strict separations are created between the development environment, the test and acceptance environment, and the production environment;
- In the processing and use of data, measures are taken to ensure the privacy of personnel and third parties. The Human Resources department may have, for example, its own network drive that is not accessible to other departments.

Integrity refers to being correct or consistent with the intended state of information. This means data cannot be edited in an unauthorized way. For example, if an employee leaves an organisation, then in that case data for that employee in all departments like accounts, should be updated to reflect status JOB LEFT so that data is complete and accurate and in addition to this only authorized person should be allowed to edit employee data. Integrity measures are:

- Changes in systems and data are authorized. For example, one member of staff in a new price for an article on the website, and another verifies the correctness of that price before it is published.
- Where possible, mechanisms are built so employees use the correct term. For example, a customer is always called a ‘customer’, the term ‘client’ cannot be entered into the database;
- Users’ actions are recorded (logged) so that it can be determined who made a change in the information;
- Vital system actions, for example installing new software, cannot be carried out by just one person. By segregating duties, positions and authorities, at least two people will be necessary to carry out a change that has minor consequences.

Availability – means information must be available when needed. For example, if one needs to access information of a particular employee to check whether employee has outstanded the number of leaves, in that case it requires collaboration from different organizational teams like network operations, development operations, incident response and policy/change management. Denial of service attack is one of the factor that can hamper the availability of information.

The *characteristics of availability* are the following: timeliness (the information is available when needed), continuity (the staff can caryy on working in the event of failure), robustmess (there is sufficient capacity to allow all staff on the system to work). Examples of availability measures include:

- The management and storage of data is such that the risk of losing information is minimal. Data is, for example, stored on a network disk, not on the hard disk of the PC;
- Back-up procedures are set up. The statutory requirements for how long data must be stored are taken into account. The location of the back-up is separated physically from the business in order to ensure the availability in cases of emergency;
- Statutory requirements for how long data must be stored will vary from country to country in EU, the USA, Ukraine, and elsewhere. It is important to check the individual government regulatory agencies for specific requirements.

Apart from this there is one more principle that governs information security programs. This is Non repudiation. *Non repudiation* – means one party cannot deny receiving a message or a transaction nor can the other party deny sending a message or a transaction. For example, in cryptography it is sufficient to show that message matches the digital signature signed with sender's private key and that sender could have a sent a message and nobody else could have altered it in transit.

Data Integrity and Authenticity are pre-requisites for Non repudiation. Authenticity – means verifying that users are who they say they are and that each input arriving at destination is from a trusted source. This principle, if followed, guarantees the valid and genuine message received from a trusted source through a valid transmission.

At the core of Information Security is Information Assurance, which means the act of maintaining CIA of information, ensuring that information is not compromised in any way when critical issues arise. These issues are not limited to natural disasters, computer/server malfunctions etc.

1.2. Computer Security. Difference between Cyber Security and Information Security

Computer security is a set of telecommunication and informatics problems related to the assessment and control of risks arising from the use of computers and computer networks and considered in terms of confidentiality, integrity and accessibility.

The Law of Ukraine “On the Fundamental Principles of Cybersecurity of Ukraine” provides the following definition: “Cybersecurity is the protection of vital interests of the individual and the citizen, society and the state in the use of cyberspace, which ensures sustainable development of the information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to Ukraine's national security in cyberspace” [8].

Creating secure computer systems and applications is the goal of network engineers and programmers, as well as the subject of theoretical research in both telecommunications and computer science, and the economy. Due to the complexity of most processes and methods of protecting digital equipment, information, and computer systems from inadvertent or unauthorized access, vulnerabilities of computer systems make a significant problem for their users. Cybersecurity is part of any organization's information security. The terms Cyber Security and Information Security are often used interchangeably. As they both are responsible for security and protecting the computer system from threats and information breaches and often Cybersecurity and information security are so closely linked that they may seem synonymous and unfortunately, they are used synonymously. Common area, that appers when cyber security and information security overlap is represented on Figure 1.3.

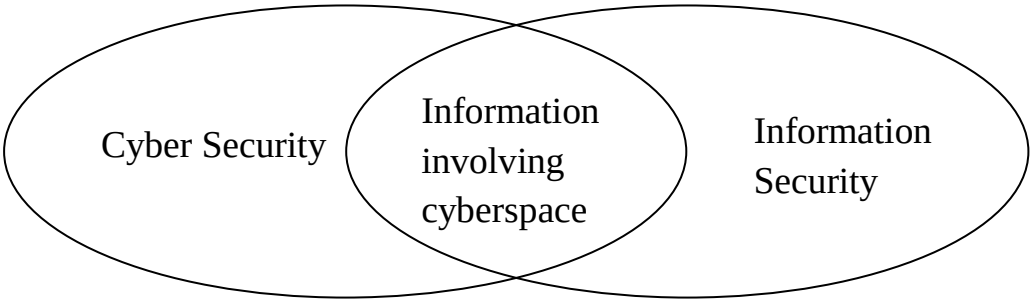

Fig. 1.3. Common area for Cyber and Information security

If we talk about data security it's all about securing the data from malicious user and threats. Another question is that what differs Data from the Information. So, one important point is that "not every data can be an information" data can be informed if it is interpreted in a context and given meaning. For example "100797" is data and if we know that it is the birth date of a person then it is information, because it has some meaning. Table 1.1 represents the difference between cyber security and information security.

Table 1.1.

Difference between cyber security and information security

CYBER SECURITY	INFORMATION SECURITY
Process of guaranteeing that computer data is defended from unauthorized digital attack, access or gamage by means of implementing several processes, practices and technologies.	The process of protecting information from unauthorized user, access and data modification or removal in order to provide confidentiality, integrity, and availability.
Deals with danger against cyberspace.	Deals with the protection of data from any form of threat.
Cybersecurity strikes against Cyber crimes, cyber frauds and law enforcement.	Information security strives against unauthorised access, disclosure, use, modification, disruption or destruction.
Cyber security professionals perform data recovering, reporting security metrics and install antimalware software.	Information security professionals find strategies, policies, solutions and perform risk management.
It deals with cyber threats such as phishing, baiting, data breach, etc.	It deals with all sorts of threats to make sure proper security protocols are in place.
Applied to digital information.	Applied to physical and digital information.

While cyber security is about securing things that are vulnerable through ICT, it also considers that where data is stored and technologies used to secure the data. Part of cyber security about the protection of information and communications technologies – i.e. hardware and software, is known as ICT security. Following Venn diagram (Figure 1.4.) can be helpful to understand the differences [9].

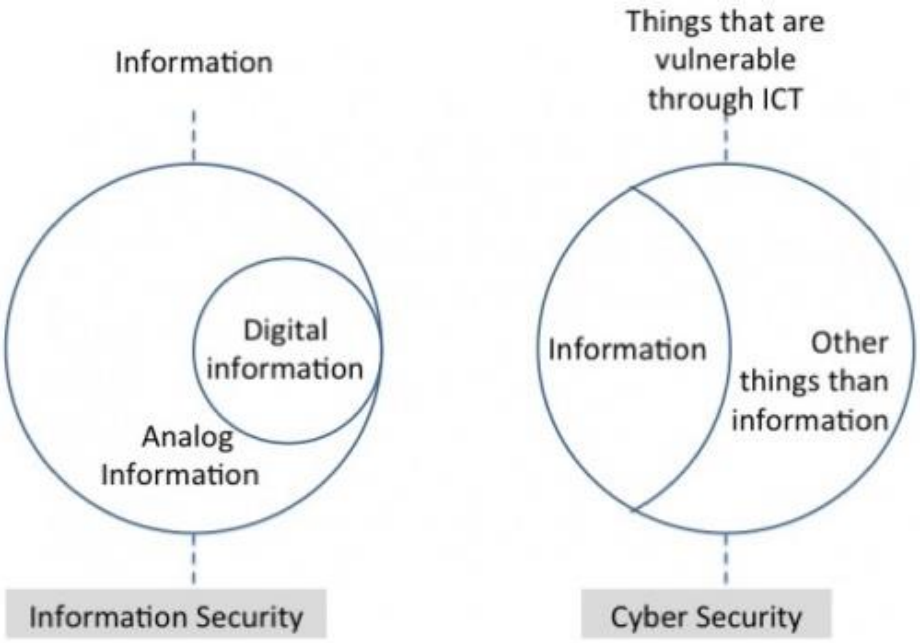

Fig.1.4. Difference between Information Security and Cyber Security

In Figure 1.5. represents that ICT refers for Information and communications technology (ICT) which is an extensional term for information technology (IT) that define the role of unified communications and the integration of telecommunications (basically digital communication security).

In the Figure 1.5, we can see that right side Venn diagram represents the Cyber security (things which are vulnerable through ICT, it includes information, both physical and digital, and non-information such as cars, traffic lights, electronic appliances, etc.), while left side represents the information security (which consist of information both digital and analog).

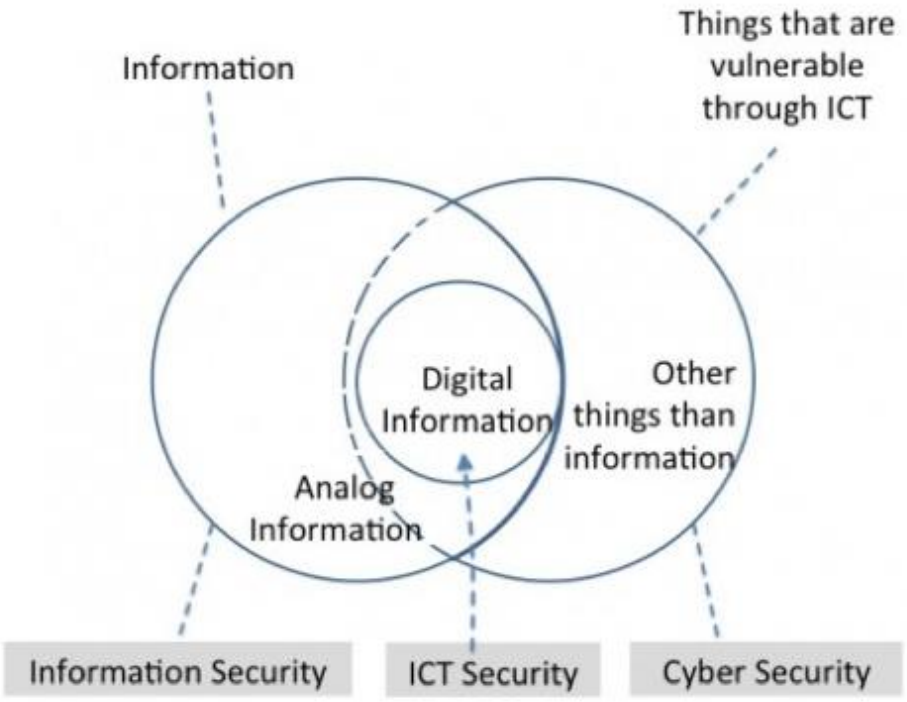

Fig.1.5. Diagram of information types

Note, that IT security is the protection of information technologies. Practically, there is no difference in ICT security and IT security. As you can see in following picture that both sets are have an overlap. Below diagram illustrates the relationship between ICT security, cyber security and information.

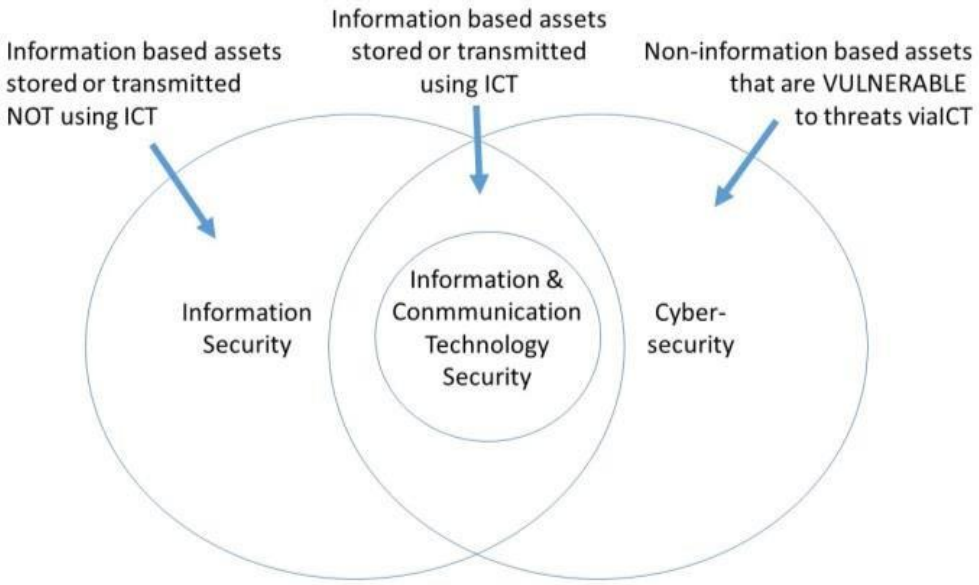

Fig. 1.6. Information and non-information based assets transmittion using and not using ICT

Figure 1.6. represents the Information & communication Technology Security that has been developed on the overlap of Information Security and Cyber Security.

1.2.1 Motives behind cyber attacks

There are various reasons that motivate cyber attacks. Sometimes it's obvious: profit is quite clearly the motive. Then again, what seems obvious might be deceptive. A simple profit motive scenario can be a smokescreen hiding a different, deeper kind of attack. Here we present some broad categories of motivation and offer high-level recommendations for mitigating the major attack vectors used.

Espionage. Usually associated with a nation state or corporate entity, espionage attacks are typically aimed at gathering information from the victim. Attacks motivated by espionage can be defined as having a reconnaissance phase in which the attackers seek the vector most likely to yield access to systems and information. The initial vector may be indirect, for example exploiting a known and trusted third party such as a disgruntled employee with access to the target system. Once inside the system, attackers usually have to move laterally through an organization's systems and gain sufficient rights to allow them access to the company's data stores or repositories. They locate their primary objective — CAD diagrams for a new aircraft design, for instance — and then exfiltrate the target data and move on to secondary objectives. An example of such an attack is the breach of Sony Pictures Entertainment, for which the attackers had multiple objectives [10]. At this point they could exit the systems and cover their tracks, or try retaining access through a backdoor created for later use. If they succeed either way, the target organization might never know that its defenses have been penetrated [11].

Profit. Direct financial gain is the aim of profit-motivated attacks and the driver behind the most active areas of cybercrime. Profit-driven attackers abound and their methods vary widely. A common profit-driven attack in use today is ransomware, covered in detail by IBM X-Force® Research report What You Need to Know About Ransomware [12].

Politics or social justice. The motivation behind cybercrimes committed by hacktivists like the Anonymous Collective is political or social. Political motivation also drives most nation-state actors. Politically motivated attackers seek mainly to acquire secret or sensitive information of one sort or another, but sabotage is another very real objective, especially in times of heightened tensions or military conflict. Nation states may also perpetrate attacks designed to damage another nation's economy [13]. Many groups outside the government sphere claim political motivation for their attacks, but it might be more accurate to call them ego- or vanity-driven. A political goal may be stated, but often they attack at random, purely to deface a victim's website by displaying their own images. They also incline towards grandiose, demonstrably false claims [14].

Patriotic or ideological motives. One class of attacker operates primarily from a perspective of patriotism or ideology, perhaps spurred into action by political and social events or motives such as revenge. There are many documented cases of attacks attributed to politically motivated attackers from countries such as the United States, Russia, China, Ukraine, Indonesia, India, Pakistan and Australia. Such attackers may not be directly politically motivated however; a state political organization may encourage such attackers [15].

Sabotage. Every year articles are published on how the power grid and air traffic control, water or other critical systems are vulnerable to attack by hackers and nation states. Typically attackers in this category seek to damage or disrupt infrastructure and critical systems for various reasons — state-operated cyber groups to reduce an adversary's effectiveness, extortionists for money, malicious actors purely for their own self-gratification [16].

Extortion. While the motivation for most ransomware extortion attacks is usually simple — profit — other extortion attacks may seek different rewards. One involves the attacker using an element of the victim's personal information, ideally something embarrassing, to coerce him or her into acting on the attacker's behalf.

Ego or vanity. Attackers motivated by vanity or ego seek fame or infamy, through cyber attacks. They might try to legitimize their obsession under the banner of a

political or social cause, but in reality they just want to see their name up in lights. Although they claim to target specific entities, typically they use vulnerability scanning tools to identify hosts that are easy to attack [17].

Revenge - the disgruntled ex-employee is one of the most easily identifiable attackers motivated by revenge. This person may still have active credentials to access their target's resources, or has retained corporate documents, that may be sold or made public. All scenarios are detrimental to the target.

1.3. Airports and airlines as critical infrastructure

Critical Infrastructure Objects - enterprises and institutions (regardless of ownership) in such sectors as energy, chemical industry, transport, banks and finance, information technology and telecommunications (electronic communications), food, health, public utilities, are strategically important for the functioning of the economy and security of the state, society and the population, failure or destruction of which can have an impact on national security and defense, the natural environment, lead to significant material and financial and human casualties [18].

The Law of Ukraine "On the Fundamental Principles of Cybersecurity of Ukraine" uses the term "Critical Infrastructures", defining them as legal entities, whose activities are directly related to technological processes and/or the provision of services of great importance to the economy and industry, the functioning of society and the safety of the population, failure or disruption of which may have a negative impact on the state of national security and defense of Ukraine, the environment, cause and property damage and/or pose a threat to life and health.

This Law also provides an interconnected definition of a critical information infrastructure object: a communication or technological system of a critical infrastructure object, a cyberattack that will directly affect the sustainable operation of such critical infrastructure object [19].

The European Programme for Critical Infrastructure Protection (EPCIP) has been laid out in EU Directives by the Commission (EU COM (2006) 786 final). It has

proposed a list of European critical infrastructures based upon inputs by its member states.

Each designated European Critical Infrastructures (ECI) will have to have an Operator Security Plan (OSP) covering the identification of important assets, a risk analysis based on major threat scenarios and the vulnerability of each asset, and the identification, selection and prioritisation of counter-measures and procedures.

The European Union defines critical infrastructure as systems that are essential to the maintenance of vital social functions. Damage to critical infrastructure, its destruction or disruption as a result of natural disasters, terrorism, criminal activity or malicious behavior can have a significant negative impact on the security of the EU and the well-being of citizens [20].

Table 1.2.

List of ECI sectors [20]

Sector	Subsector	
I Energy	1. Electricity	Infrastructures and facilities for generation and transmission of electricity in respect of supply electricity
	2. Oil	Oil production, refining, treatment, storage and transmission by pipelines
	3. Gas	Gas production, refining, treratment, storage and transmission by pipelines LNG (liquefied natural gas) terminals
II Transport	4. Road transport 5. Rail transport 6. Air transport 7. Inland waterways transport 8. Ocean and short-sea shipping and ports	

'European critical infrastructure' or 'ECI' means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact

on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure. The list of ECI is represented in the Table 1.2.

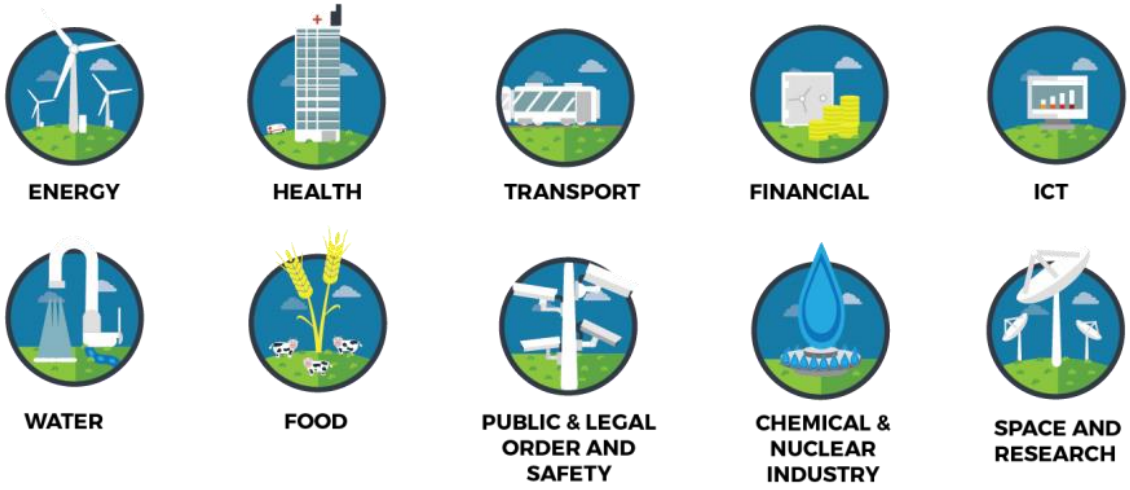

Fig. 1.7. Systems that fall under such CI sectors [43]

According to the information provided by the Ministry of Infrastructure of Ukraine by letter dated 05.12.2017 No. 12571/12 / 10-17 (hereinafter - Letter from the Ministry of Infrastructure), to the field of aviation transportation include: airport, airfield, runway.

In accordance with paragraph 2 of the Procedure for establishing a list of information and telecommunication systems of critical infrastructure of the state approved by Resolution of the Cabinet of Ministers of Ukraine dated 23.08.2016 No. 563, objects of critical infrastructure - enterprises and institutions (regardless of ownership) of such industries such as energy, chemical industry, transport, banks and finance, information technology and telecommunications (electronic communications), food, health, utilities that are strategically important for the functioning of the economy and security of the state, society and population.

An infrastructure is a system that combines various facilities and enables certain activities, for example, a pipeline that brings water from wells to homes and fields, paved roads, bridges and intersections that allow movement of people and goods, flights, communications, fuel, and health services. One of the properties of an infrastructure is

the dependence of various spheres of activity on it. In the past, the dependence stemmed from physical or geographical relationships only. With the development of cyberspace, which includes data communication systems and computerized methods of automatic command and control, there are additional relationships, which in turn create further vulnerability. These are computerized relationships (for example, command and control by remote electronic means) and logical relationships (such as the international financial market as a factor influencing inputs and outputs of critical infrastructures), which are innovations that would not exist without information technologies. It is therefore worth distinguishing between infrastructures in the traditional sense and the modern use of this concept, which includes a cyber dimension.

In the information age, traditional infrastructures become information infrastructures because they incorporate computers. In addition, new critical infrastructures that are purely information infrastructures have been created: computerized databases that contain important data, such as records of capital in the banking system, scientific and technical intellectual property, and the programmed logic that manages production processes and various business processes. In the information age, the concept of "infrastructure" also includes computerized components, and thus "infrastructure" today necessarily refers to an information infrastructure. Infrastructure is defined as critical when it is believed that disrupting its function would lead to a significant socio-economic crisis with the potential to undermine the stability of a society and thereby cause political, strategic, and security consequences. Different countries have offered a variety of definitions of critical infrastructures [21]. What all have in common is the existence of a computerized element upon which other physical systems are dependent and which, if harmed, would likely cause widespread damage in physical terms [22].

Three factors that define a critical infrastructure are listed and described below.

The first is the symbolic importance of the infrastructure. Thus, several democratic countries include heritage sites, museums, archives, and monuments among critical infrastructures that should be protected from cyber threats. For example, Australia and the United States, which are countries that clearly attribute great

importance to their political history as a central element in their collective national identity and social and political strength [23]. Another source of symbolic power is the perceived control of a government. For example, a hostile disruption of traditional media used by the state for communicating with its citizens will immediately harm the government's ability to function. Moreover, in the longer term, such disruption may diminish the citizens' confidence in the existing government, or even the general form of government or regime.

The second factor is the immediate dependence on infrastructure, such as the electricity grid of telecommunications network, which is obvious for most processes in society. The emergence and prevalence of cyberspace created a situation in which computerized networks constitute an infrastructure in and of themselves. Cyberspace is a representative example of an infrastructure that has become critical because of the interface of most of society's activity with computerized communications networks.

The third factor involves complex dependencies. The accelerated trend toward adding connectivity capabilities enables unanticipated effects beyond the local level. This refers to a tenet of chaos theory describing how tiny variations affect complex systems.

The commercial aviation sector, which has attracted the attention of enemies of the developed states and prompted noticeable acts of hostility – hijacking of commercial planes, the September 11 attacks, and other terrorist attacks using civilian airplanes – can illustrate the importance of critical infrastructures and the significance of an attack on them. Civil aviation is a basic infrastructure for developed societies: in 2018, commercial air transport carried more than 2 billion passengers on 28 million flights on 27,000 airplanes operating from 3,970 commercial airports around the world [24]. In addition to commercial flights, military aircraft (some unmanned) also populate the skies. Domestic laws, regulations, and procedures, along with international cooperation, regulate the administrative aspect of the airline industry. Airports are connected to each other through regular air traffic, and the air traffic control system at each specific location is part of the international aviation infrastructure. Air traffic control is based on computerized systems such as methods of detection, monitoring, surveillance,

automation, communications, command and control, and so on. Disrupting the proper functioning of air traffic control systems would harm all air traffic.

1.4. Major information security and cyber security threats faced by airports and airlines

Recent years have brought increased concern over the potential vulnerability of the infrastructures, that are the basis of developed modern societies. The United States was a pioneer in this field, initiating a discussion of the presidential level in 1996: United States, President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection (Washington, D.C.: U.S. G.P.O., 1997). Yet the fact that this discussion is still taking place now is surprising.

Critical infrastructures have always been critical and their importance is obvious. International and internal conflicts are not new to the world, and in war it is reasonable to anticipate attempts to harm the adversary's critical infrastructures with the goal of weakening and defeating it. In 1917, during the Bolshevik Revolution, Lenin and Trotsky ordered their activists to take over the post office, telegraph systems, bridges, and train stations. In prolonged wars, such as the Second World War, attempts have been made to harm critical infrastructures in order to interfere with the enemy's fighting ability and spirit. In the "strategic bombing campaign" in World War II, the allies concentrated their aerial effort on attacking German factories producing ball bearings and lubricating oils, refining facilities, and railroad junctions. The operation was intended to harm the critical infrastructure for weapons manufacturing.

A country's critical infrastructures, whatever they are, are elemental targets during a conflict, and therefore organizations and states have labored throughout history over defense systems for their infrastructures: camouflage, guarding, fortification, defensive forces, deterrence, and so on. However, there are reasons for fear of damage to critical infrastructures, particularly in the strongest countries.

In all forms of traditional warfare, the identity of the enemy is disclosed following the attack because, in order for the attack to be carried out, the weapons must physically reach the target. In the event of a missile launch as well, there is no doubt as to the location of the launch site. The hijacking of commercial aircraft in the 1970s, the suicide bombings in Israeli population centers, the attacks in the United States in September 2001, and the attacks in Madrid in 2004 and London in 2005 all required the attackers to be physically present at of the attacks.

Identifying the enemy is critical for response and deterrence. Thus, what prevented harm to critical infrastructures in the past was the defensive force placed in the path of the enemy, and even more so, the deterrence that promised to exact a heavy price. This familiar state of affairs came to an end with the development of cyberspace. For the first time in history, it is possible to attack strategic targets (such as critical infrastructures) without physically being in the place where they are located, without confronting defensive forces, and without exposure. In today's reality, the existing computerized infrastructure can be exploited through penetration of communications networks or the software or hardware of the command and control computers in order to disrupt, paralyze, or even physically destroy a critical system. The feasibility of using cyber means to cause physical damage has been shown in experiments. A CNN broadcast that discussed the Aurora experiment, ordered by the US Department of Homeland Security and conducted at Idaho National Labs, noted that broadcasting instructions to the command and control system of the electricity generating system caused a generator to stop working and then to explode. The threat stems from the vulnerability inherent in the properties of cyberspace, and because of these special characteristics, the cyber threat challenge differs fundamentally from the challenges of traditional threats.

Following is a summary of the challenges stemming from the characteristics of cyberspace as it exists today: the major vulnerability of computerized systems; the difficulty in distinguishing between a glitch and an attack, making the connection between an event and the result, tracing the source of the damage, and identifying the

attacker, even if the source of the damage is known; and the widespread use of off-the-shelf commercial technologies [25].

There is tremendous pressure to strengthen end-to-end security and to do so swiftly. The major challenges faced by airports and airlines are represented in the Figure 1.8 and described below:

- Siloed legacy systems make it difficult to implement streamlined end-to-end security;
- Too much connectivity: physical assets, including scanners, access and departure control, and security cameras are now connected to an airport's or airline's systems, making it easier for a cybercriminal to get access to physical equipment. With the explosion of IoT devices new opportunities arise but also, and more importantly, new challenges appear, connected to the inherent lack of security within these devices. An IoT device is a piece of hardware with a sensor that transmits data from one place to another over the Internet. Types of IoT devices include wireless sensors, software, actuators, and computer devices;

Fig. 1.8. Major challenges faced by airports and airlines [44]

- A quickly evolving threat landscape, with criminals using increasingly sophisticated tools which might challenge existing cybersecurity budgets, particularly at

smaller airports. While those smaller airports will certainly comply with existing regulations, there is no doubt that their ability to implement the latest security technologies is going to be lower than at a major international airport. This will generate a disparity amongst airports in the methods and degree to which cybersecurity is addressed, some of them having a very mature cybersecurity posture while others will have limited capabilities;

- Multiple regulations coming from local, regional and global organizations make it difficult to keep up with compliance;
- A complex ecosystem of stakeholders, with massive data flows moving among the different parties, with the volume, velocity and variety of the data quickly increasing. Big Data solutions are becoming ever more necessary in order to properly manage both the unstructured and structured data that is being generated, processed and stored within this complex ecosystem.

1.5. Overview of countries' cyber security policies

Critical Infrastructure security is of paramount importance in protecting assets and services that are essential to society and the economy. The real-world, high profile consequences of a cyber-attack could include service disruption, environmental damage and personal injury on a large scale. Alongside this, there is the often mammoth task of managing a large number of customers, and handling data relating to usage, payments and connection status. If you work in one of these sectors you know that your operations must be high performing, resilient and secure. A strong cyber security posture is fundamental to your operation.

There is considerable pressure on critical infrastructure, from advisory groups and national governments – for example through Centre for Protection of National Infrastructure (CPNI) in the UK, the Australian Government's Critical Infrastructure Centre (CIC) and via the North American Electric Reliability Corporation (NERC) in the US.

1.5.1. The Cyber Security Policy of EU

Cybersecurity Strategy of The European Union: An Open, Safe and Secure Cyberspace was presented by European Commission (EC) on February 7th, 2013. The strategy seems to be based on the action plan of ‘Digital Agenda for Europe (DAE)' presented as EU's comprehensive cyber security strategy in 2010. DAE consists of 101 actions plans of 7 fields. 13 action plans out of 101 are related to cyber security. Additionally, the government placed 7 action plans on top priority tasks. The Cybercsecurity Strategy of The European Union can be evaluated as one of the achievements of the 7 action plans [27].

The Cyber Security Strategy presents 5 specific action plans and coordination scheme formation, consisting of stake-holders in related public-private organizations such as EC, ENISA(European Union Agency for Network and Information Security) and EC3(European Cybercrime Center) in oder to carry out the 5 plans.

Network and Information Security (NIS), which is enforceable to successfully carry out the plans with Cyber Security Strategy, was suggested. The NIS, aiming at the protection of information security by setting up unified EU standard, regulates the monitoring of online stability and the establishment of CERT.

Moreover, ENISA established to support EU members's information security measures in 2004 plays an important role in the enforcement and management of various measures based on the NIS. Recently, ENISA presented National Cyber Security Strategies: Setting the course for national efforts to strengthen in Cyberspace as a security strategy guideline for member states in May 2012 [28]. Also, National Cyber Security Strategies: Practical Guide on Development and Execution was introduced in December, the same year [29]. Moreover, thanks to the foundation of the regulation of strengthening of function in June 2013, cyber security policy and legal institution related supports were expanded for ENISA. As a result, its right of intervention into member states' policy and institution was expanded as well [30].

For public-private cooperation of the EU, EP3R (the European Public-Private Partnership for Resilience), based on ENISA as an information sharing network, was

established. E3R is a framework that encourages both of government and private sectors to participate in policy making and strategic decision making for critical infrastructure protection and resilience strengthening [31]. Essentially, E3R aims at the construction of environment for trusted collaboration. For this, so called Voluntary Self-regulation system, which allows only limited member' participation, is applied. However, it is expected that EU also change its way to Enforced Self-regulation after the authority of E3R becomes strengthening with the enforcement of cyber security strategy and NIS.

New legislation includes EU Directive 2016/1148 on the security of network and information systems (NIS) which took effect across Europe and in the UK on 10 May 2018. This Directive places requirements on providers of essential services in a number of critical national infrastructure sectors and aims to enhance the security and resilience of networks and IT systems across the EU.

European Civil Aviation Conference Doc 30 declares that measures addressing cyber threats to CA have been included in the National Civil Aviation Security Programme, the National Quality Control Programme and the National Civil Aviation Security Training Programme. A set of security control consists of below measures [32]:

1) Implementation of effective measures to protect Critical Aviation Information Systems (CAIS);

2) Including the CAIS in their threats assessment processes;

3) Separating the CAIS networks from public;

4) Responsibility for securing CAIS is allocated by operators to a properly selected, recruited and trained individual;

5) Security measures are considered in the design, implementation, operation and disposal of new CAIS;

6) Supply chain security measures for hardware and software should be applied to CAIS;

7) Remote access to CAIS is only permitted under pre-arranged and secure conditions;

8) Cyber attack incidents must be recorded for future evaluation and counter & preventive measures efficiency increasing.

It is also worth noting that the most comprehensive list of measures to mitigate cyberthreats' negative influence on CAIS there is in ICAO Doc 8973 [33]. Among them is noted as follows:

- Administrative Measures;
- Virtual (Logic) Control Measures;
- Physical Controls.

Besides this document, also focuses of CAIS: security by design, networks separation & secured remote access for legitimate users, supply chain security & cyber attack incidents records.

The 14 High Level Security Principles proposed by the UK government to meet the security requirements of the NIS Directive include an effective security monitoring strategy and proactive security event discovery. Operators of essential services in the UK are currently encouraged to start analysing their systems and existing security measures to identify control gaps and plan any necessary remediation.

1.5.2. The Cyber Security Policy of the US

The current cyber security policy of the US is based on Comprehensive National Cybersecurity Initiative (hereafter, CNCI) implemented by Bush administration on January 8th, 2008. Additionally, Obama administration which started in January 2009, put cyber security policy at the top of its agenda and presented (Cyberspace Policy Review (CRP) in the same year [26]. Currently, various cyber security policy of the US is based on the CRP.

CRP suggests 10 short-term tasks and 14 mid-term tasks and also presents the establishment of effective information sharing and emergency response system as short-term projects. This project, followed by National Cyber Incident Response Plan (NCIRP) presented by the Department of Homeland Security in September, 2010, paved way for the establishment of public-private information cooperation system. NCIRP, focusing on the development of response mechanism for 'critical cyber infringement accident', is aimed for the establishment of strategic framework such as the role and responsibility of

organization, action plan, countermeasures and recovery plan to response cyber infringement accident.

Taking 9.11 as a momentum, US government included major infrastructure as a target of cyber threat and started dealing with this issue as national security and implementing related executive order. In March 2003, US government integrated exiting multiple departments charged of the protecting of infrastructure into one organization, the Department of Homeland Security, which is exclusively responsible for the protection of national infrastructure under Homeland Security Act enacted in November, 2002.

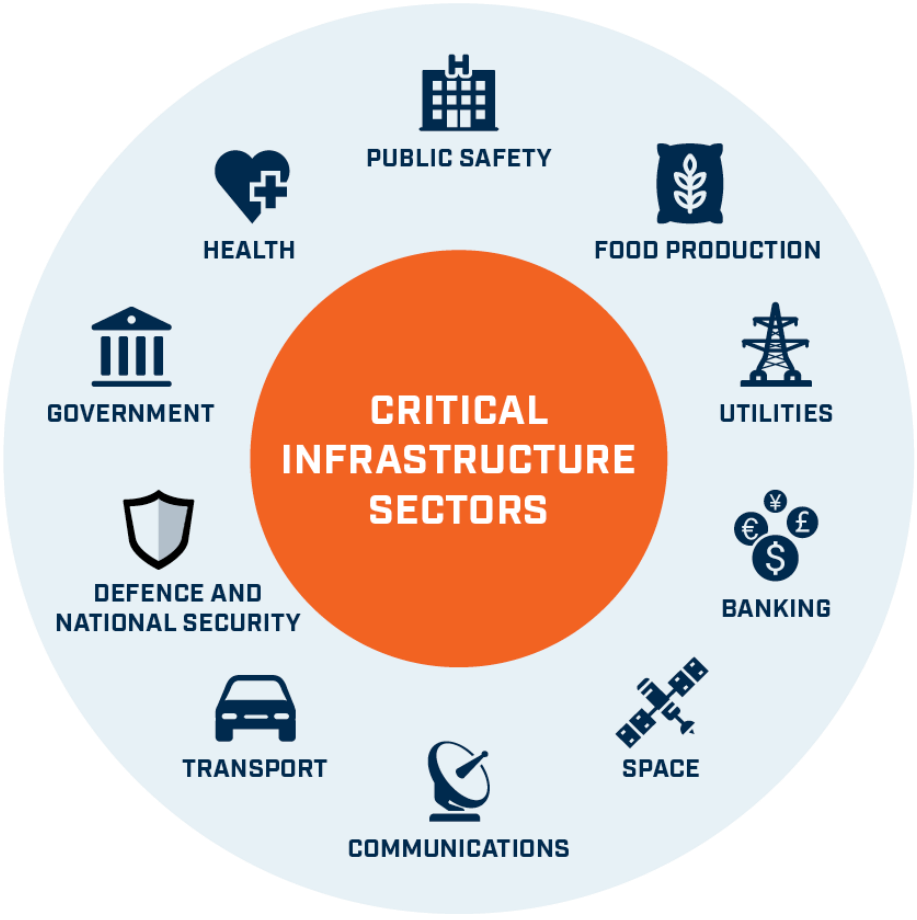

Fig. 1.9. Critical Infrastructure Sectors in the USA

Regarding public-private information cooperation, Executive Order 13636 for Improving Critical Infrastructure Cybersecurity signed by president Obama was presented in February, 2013. The executive order defines several things as follows. Firstly, it requests the Ministers of Homeland Security, Judiciary, National Information

and Defense to voluntarily share information about cyber threat as a measure of information sharing in this field. Secondly, it requests the Department of Homeland Security to lead to form consultative group about the cyber security of critical infrastructure with stake-holders. Furthermore, under the leadership of National Institute of Standards and Technology (NIST), Baseline Framework to Reduce Cyber Risk to Critical Infrastructure was developed. However, the executive order has no right to establish and introduce framework, but only aims to support each organization to reinforce voluntary cyber security.

The degree of US government intervention in regard to cyber security policy and related public-private partnership are now based on Voluntary Self-regulation, and US government also try to remove obstacles for the promotion of self-regulation. Additionally, various information cooperation system and support organization were established under the leadership of the Department of Homeland Security.

Cybersecurity Capability Maturity Model (C2M2) proposed in North America. The C2M2 is a voluntary public-private partnership program, the development of which is not associated with any compliance requirements. The C2M2 model was identified, organised, and documented by US energy sector subject matter experts from both public and private organisations. The C2M2 is designed to measure both the sophistication and sustainability of a cyber security program.

1.5.3. Cyber Security Policy of Japan

Japan started to organize functions and system related to information security issues in order to strengthen government-centered system by reexamining government roles and functions regarding the issue in December, 2004. Furthermore, in April 2005, Japan also established National Information Security Center (hereafter, NISC) as the control tower of information security under the authority of government. NISC is responsible for forming national information security strategy and plays a role as all-source situation room under an emergency situation. Moreover, it also establishes safety

standard which set up the level of protection measures for critical infrastructure and manages CEPTOAR-Council aiming at public-private cooperation as well.

Japan suggested the basic idea and policy direction of information security by establishing The First National Strategy on Information Security: Toward the creation of a trustworthy society in 2006. After this, Japan has been continuously establishing and modifying information security strategies, and finally founded cyber security strategies in 2013. In this strategy, the target area of protection was expanded to cyber security strategy recognizing the importance of cyberspace from information security centered strategy. Also, Japanese cyber security strategies have a lot in common with those of the US such as the establishment of public-private cyber security standard and the formation of information sharing system among stake-holders. Besides this, Japan also tries to exercise global leadership by presenting j-initiative for Cybersecurity. Especially, Japan also makes an effort to contribute to the formation of international cyber security standard.

In case of Japan, the degree of government intervention is defined by Voluntary Self-regulation and each government department manages public-private cooperation system. For instance, the Ministry of Internal Affairs and Communications organizes public-private council, so-called Telecom-ISAC Japan with communicative enterprises and the Ministry of Economy, Trade and Industry also manages information cooperation system with people engaged in manufacturing industry through Initiative for Cyber Security Information sharing Partnership of Japan(J-CSIP). In this case, each government department promotes its own cooperation with private sectors case-by-case..

1.6. Aviation information security audits

On the basis of Assembly Resolution A33-1 adopted in 2001 and the recommendations of the High-level, Ministerial Conference on Aviation Security (Montreal, February 2002), the Council adopted in June 2002 the Aviation Security Plan of Action, which included the establishment of a comprehensive programme of regular, mandatory, systematic and harmonized audits to be carried out by ICAO in all

Contracting States. The ICAO Universal Security Audit Programme (USAP) was subsequently launched, with the objective of all Contracting States having benefited from an initial audit by the end of 2007.

The ICAO USAP has been implemented on schedule and within its budget allocation. The audits have proven to be instrumental in the identification of aviation security concerns and in providing recommendations for their resolution. From its inception, the USAP has enjoyed the support of Contracting States and is promoting positive change as States become increasingly sensitized to the international requirements. The USAP follow-up missions have validated a markedly increased level of implementation of ICAO security Standards, thereby attesting to States' commitment to achieving the objective of the USAP to strengthen aviation security worldwide. A security culture, if such were to exist among ICAO's member States, would mean that the States would be aware of their rights and duties, and, more importantly, assert them. Those who belong to a security culture also know which conduct would compromises security and they are quick to educate and caution those who, out of ignorance, forgetfulness, or personal weakness, partake in insecure conduct. This security consciousness becomes a "culture" when all the 190 member States as a whole makes security violations socially and morally unacceptable within the group.

All ICAO Member States are to were successfully audited by the end of 2007, with strengths and weaknesses identified, regional and global trends tracked, and recommendations made to States for improving their security regimes. Although security audit information has been restricted in the past, steps should be taken to increase the transparency of the audit programme and ensure that the global aviation network remain protected. It is therefore proposed that, in addition to a review of deficiencies by the Audit Results Review Board, consideration be given to the development of a process that will notify all Member States when deficiencies identified during the course of a USAP audit remain unaddressed for a sustained period. A notification process could involve the use of information which does not divulge specific vulnerabilities but enables States to initiate consultations with the State of interest to ensure the continued protection of aviation assets on a bilateral basis.

Comprehensive statistical analysis of audit results and levels of compliance (globally, by region, and by subject matter) is available on the USAP secure website. Key findings are presented at both the national and airport levels. According to the progress report submitted to the ICAO Council in 2006 the ICAO Secretariat advised that in the case of States that are demonstrating little or no progress by the time of the follow-up visit, a cross analysis of the USAP audit results with those of the USOAP reveals that generally, States that have difficulty in implementing the safety-related SARPs are also experiencing difficulties with the implementation of the Annex provisions on the security side. Certain contributing factors have been identified. These often include a lack of financial and/or suitably qualified human resources as well as frequent changes in key personnel within a State's Appropriate Authority. In certain cases, there also appears to be a certain complacency and general lack of interest in implementing the ICAO recommendations.

In order to address the issue of States that are not responding effectively to the ICAO audit process, a high-level Secretariat Audit Results Review Board has recently been established for the purpose of examining both the safety and security histories of specific States brought to its attention by either ICAO's USOAP of USAP. The objective would be is to highlight or raise the profile of these States within the system in order to encourage them to take responsible actions in a measured and timely manner [34].

The Committee on Unlawful Interference of the ICAO Council has recommended to the Council that these data and trends be made public at the Assembly. Although such information has been restricted in the past, the Committee believes all States and the public should be aware of the areas needing improvement without identifying specific States or vulnerabilities. While reports show that many ICAO Member States have actively used information gathered from USAP audits to improve their security systems, reports also demonstrate that other States cannot or will not make necessary changes. For those States that lack resources to improve their security systems, new mechanisms such as ICAO's Coordinated Assistance and Development (CAD) Programme are in place to assist in directing longer-term attention to problems.

1.6.1. Security Oversight

Aviation Security oversight is the means by which States ensure effective implementation of their national security requirements in compliance with the security - related related Standards and Recommended Practices (SARPs).

Critical Elements of a State ’s Security Oversight System are:

CE 1: Aviation Security Legislation

CE 2: Aviation Security Programmes and Regulations

CE 3: State Appropriate Authority for Aviation Security and its Responsibilities

CE 4: Personnel Qualifications and Training

CE 5: Provision of Technical Guidance, Tools and Security Critical Information

CE 6: Certification and Approval Obligations

CE 7: Quality Control Obligations

CE 8: Resolution of Security Concerns

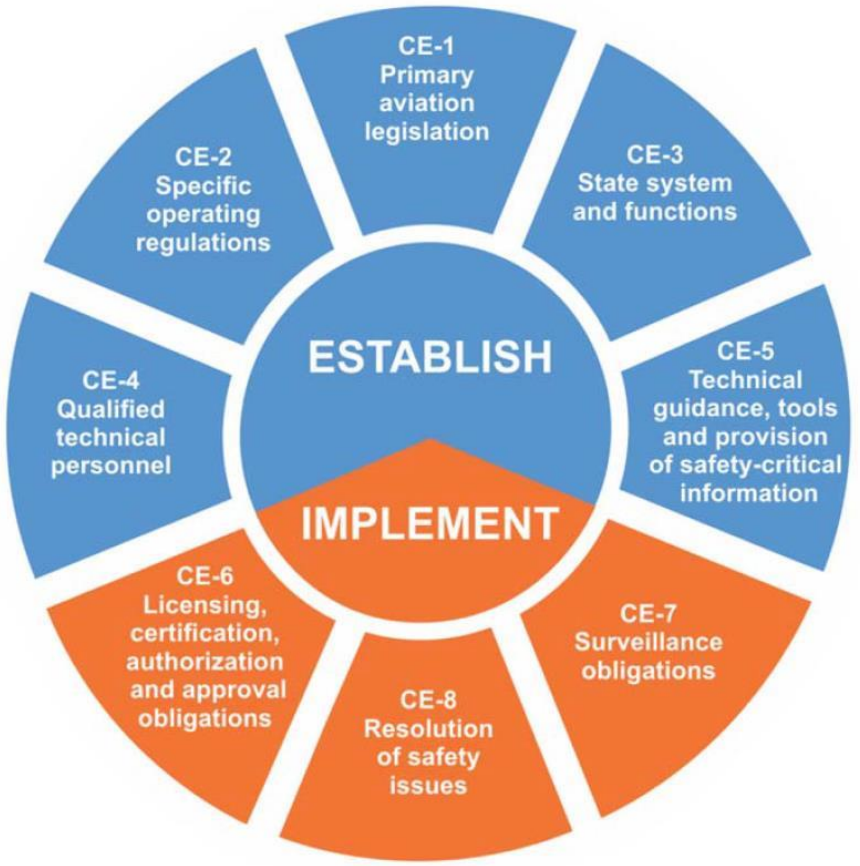

Fig. 1.10. Critical elements of a state’s Security oversight system

ICAO has a security oversight programme called the Universal Security Audit Programme (UASP). The ICAO Universal Security Audit Programme (USAP), launched in June 2002, represents an important initiative in ICAO's strategy for strengthening aviation security worldwide and for attaining commitment from States in a collaborative effort to establish a global aviation security system.

The programme, which is part of the Aviation Security Plan of Action, provides for the conduct of universal, mandatory and regular audits of the aviation security systems in all ICAO member States.

The objective of the USAP is to promote global aviation security through auditing Contracting States, on a regular basis, to determine the status of implementation of ICAO security Standards.

The primary objectives of an ICAO security audit are to:

a) determine the degree of compliance of the State in implementing Annex 17 Standards and security-related provisions of Annex 9;

b) observe and assess the State's adherence to associated security procedures, guidance material and security-related practices;

c) determine the sustainability and effectiveness of the State's implementation of a security system, through the establishment of legislation, programmes, regulations and a security authority with control and enforcement capabilities;

d) determine the State's capability for security oversight by assessing the effective implementation of the critical elements of a security oversight system; and system; and

e) provide recommendations to Contracting States to improve their security systems and oversight capabilities.

Since the launch of the USAP in 2002, 169 aviation security audits and 77 follow-up missions have been conducted. ICAO performs comprehensive analysis of audit results on levels of compliance with Annex 17 – Security Standards on an ongoing basis (globally, by region and by subject matter). This statistical data is made available to authorized users of the USAP secure website and is shared with other relevant ICAO offices as a basis for prioritizing training and remedial assistance projects. As of 31 July

2007, 77 follow-up missions had been conducted. These missions take place two years after the initial audit with the purpose of validating the implementation of State corrective action plans and providing support to States in remedying deficiencies. These missions are normally conducted by the applicable Regional Office, with close coordination through Headquarters. The results of the follow-up visits indicate that the majority of States have made significant progress in the implementation of their corrective action plans.

USAP offers audit assistance for both pre-audit and post-audit periods [35]:

Table 1.3.

USAP audit assistance

Pre-Audit Preparation	- development of Inception Report; - highlighting the status of Protocol Question across all Critical Elements and providing guidance to pre-audit questionnaires and compliance checklists; - pre-audit documentation preparation.
Post-Audit Assistance	- review of USAP findings; - development of a Corrective Action Plan (CAP); - corrective action technical assistance to rectify any security oversight deficiencies identified in the USAP audit; - development of appropriate security regulatory frameworks for long-term; - sustainable compliance with national and international best practice capacity building and training to ensure regulatory and inspectorate staff are competent carrying out security oversight functions.

A high-level ICAO Secretariat Audit Results Review Board (ARRB) has been established as part of an overall coordinated strategy for working with States that are found to have significant compliance shortcomings with respect to ICAO Standards and Recommended Practices (SARPs). The ARRB examines both the safety and security

histories of specific States and provides an internal advisory forum for coordination among ICAO's safety, security and assistance programmes.

USAP Characteristics are the following:

- Regular, mandatory, systematic and harmonized audits;
- Evaluation of aviation security in place in all 190 ICAO Contracting States;
- Audit State Audit State's aviation security oversight capability s aviation security oversight capability;
- Audit security measures at selected airports;
- Funded by voluntary contributions

Preparing for an ICAO USAP audit can be a complex process, especially when a State lacks security oversight knowledge or resources. We can provide UK CAA best practice advice across all aspects of the ICAO audit process to help States achieve security compliance with the ICAO standards.

Audit Related Documents that are used at USAP audit process:

- Chicago Convention;
- Annex 17 to the Chicago Convention: Standards;
- Annex 9 to the Chicago Convention: Security – related Provisions;
- Security Manual Security Manual – Doc 8973;
- Security Audit Reference Manual – Doc 9807 Doc 9807;
- Oversight Manual – Doc 9734 Part C

1.6.2. ECAC Aviation Security Audit Programme

The primary objective of the ECAC Aviation Security Audit Programme is to assess the implementation of Doc 30 Recommendations in ECAC Member States. As a more global objective, these audits contribute to more effective implementation of international standards by ECAC Member States and to the harmonisation of security measures among these States. Furthermore, the creation of a common security area can only be achieved by the full implementation of Doc 30 Recommendations by all

Member States. Participation in the ECAC Aviation Security Audit Programme (hereinafter "the Programme") facilitates the development of one-stop security arrangements between all ECAC Member States.

The objectives of the Programme are:

- to assess the implementation of Doc 30 Recommendations;
- to identify areas of needed improvement and provide Appropriate Authorities with advice and technical expertise;
- to provide Member States with capacity building activities to meet Doc 30 Recommendations;
- to facilitate the development of one stop security arrangements.

ECAC aviation security audits are conducted based on an approved Audit Methodology. Participation in the Audit Programme is entirely voluntary and starts with a Memorandum of Understanding between ECAC and each participating State. The audits are based on interviews, the review of documentation and thorough on-site observations. In accordance with the recent changes to ECAC Audit Methodology, the Member States can decide to be subject to either a comprehensive audit covering all Doc 30 Recommendations or a thematic audit focusing on a particular area of aviation security.

The audit team provides an interim report to the Appropriate Authority on the last day of the audit and a final report with relevant details 60 days later. Initial and follow-up audits are conducted and States provide Action Plans to address deficiencies identified. Recently, a new type of aviation security audit has been introduced with a focus on the assessment of the aviation security oversight system in Member States. Its main objective is to verify whether the existing national legislation and procedures allow Member States to perform efficiently their oversight functions in the field of aviation security.

The ECAC security audit and capacity-building activities available to Member States to support their implementation of aviation security measures are compiled in a catalogue.

Auditor training and certification

ECAC auditors are certified to assure Member States of their knowledge and expertise. The pass mark to be achieved from five different competency tests is 70%. Member States nominate individuals to participate, and cover their costs when they are released to conduct audits. Additionally, the auditors meet annually to ensure continuous professional development and to review performance. These principles ensure the Programme's quality, transparency and independence, to the benefit of Member States.

ECAC Auditor Training and Certification lasts for seven days and includes oral and written tests. Candidates are assessed on their theoretical and practical knowledge of aviation security and competency in performing as an auditor within an international context.

Member States are invited to provide the ECAC Secretariat with nominations to participate in the ECAC Aviation Security Training and Certification all year-round, by using the form here.

The training and certification sessions are usually organised in July each year. Candidates' background and knowledge on aviation security measures are subject to verification by the ECAC Aviation Security Audit and Capacity Building Officer prior to the course. Only candidates demonstrating a good level of English and a high level of aviation security expertise will be accepted on the course.

Certified ECAC Auditors

The ECAC Aviation Security Auditors Handbook has been created to assist certified ECAC auditors in the preparation and conduct of an audit. The Handbook includes all documents that relate to the audit process, such as methodology of an audit, the Auditors Aide and templates to assist with the reporting of audit findings.

ECAC certified auditors meet annually to exchange their experience, continuous professional development and to review the latest developments in the ECAC Work Programme in the field of aviation security.

Conclusions to the theoretical part

Today, information systems play a key role in ensuring the efficiency of commercial and state-owned enterprises. The widespread use of information systems for storing, processing and transmitting information makes the problems of their protection relevant, especially given the global upward trend in the number of information attacks leading to significant financial and material losses. For effective defense against attacks, companies need an objective assessment of information system security level, which is why security audits are used.

According to analysis, the US, EU and Japan carry out strategies from the perspectives of cyber security. In the case of the EU, member states are, to some degree, different from each other but every member state recognizes the importance of cyber security policy in common. The development of ICT and the entry into smart society surely makes our lives affluent and expose us to much threat at the same time. Every state shares the same concept regarding this issue and its countermeasures are also very similar. The important features are as follows: firstly, it establishes strategies which comprehensively include cyberspace; secondly, public-private cooperation system under the authority of government tends to be strengthened in order to smoothly respond to major cyber security accident before and after the accident; thirdly, the way of government intervention into private sectors is changing to Enforced Self-regulation. This trend implies that cyber security related issues are too difficult to solve problems by completely relying on private autonomy.

Thus, the field of information security has grown and evolved significantly in recent years. It offers many areas for specialization, including securing networks and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning etc.

Cybersecurity today is responsible for three factors: systems, processes, people. Moreover, given the widespread integration of digital technology into the life and body of a person, the issue of information security becomes, at times, a matter of vital security. Thus, the old notion of information security does not address the wide range of

issues that arise in 21st Century cyberspace. Instead, information security has become part of cybersecurity as a result of evolution.

Aviation enterprises are a part of critical infrastructure. Although at first glance it appears that the subject of protecting critical information infrastructures belongs in the realm of computer engineering, upon further examination it becomes clear that it should be expanded beyond the technical aspect. Indeed, the major challenge in protecting critical infrastructures from cyber threats is not technical, but strategic and politic. In Ukraine critical infrastructure is regulated by Decree №518 dated June 19,2019 on approval of the General requirements for cyber defense of critical infrastructure and under the discussion is the Draft Law of Ukraine "On Critical Infrastructure and its Protection". Only a thoughtful, informed process can design a policy of effective critical infrastructure protection from cyber threats and thus reduce the risk confronting developed countries from cyberspace. The major recommendation, therefore, is to broaden the public discussion of cyber security to include social and cultural aspects, which will make it possible to cope with the threat optimally on a national-strategic level with a comprehensive national perspective.

2. ANALYTICAL PART

Air Transportation Management Department				*NAU 20.08.35.200 EN*			
Researcher	*Mariana Y.Khodurska*			*ANALYTICAL PART*	*Letter*	*Sheet*	*Sheets*
Supervisor	*Ivannikova V.Yu.*				*D*	*54*	*33*
Standards Inspector	*Yulia V. Shevchenko*				*FTML 275 ОП-202Ма*		
Head of the Department	*Yun G.M.*						

2.1. General characteristics of Ukraine International Airlines

Ukraine International Airlines is a privately owned Ukrainian airline that was founded as a state-owned company in 1992 and fully privatized in 2011. Ukraine International Airlines (abbreviated - UIA) was established on October 1, 1992 as a separate unit of the state Airlines of Ukraine. In English, the name of the parent airline sounded like "Air Ukraine", so the subsidiary was named "Air Ukraine International". From the first letters AUI ICAO registration code was created. Boryspil International Airport has become and remains to this day as the base airport.

The first flight was made on the route Kiev-London-Kiev on November 25, 1992. This date is considered to be the birthday of UIA. From the very beginning, Ukraine International Airlines operated its Boeing 737 aircraft, thus becoming the first aircraft operator of this type in the post-Soviet space. The next destinations after London were Frankfurt and Paris. In March 1993, the UIA route network also covered Amsterdam, Berlin, Brussels, Milan, Munich and Vienna.

In April 2011, the full privatization of the UIA Airlines took place. The State Property Fund sold the entire stake owned by the state. At that time, the shareholders of the company, except SPFU, were: Austrian Airlines (22.52%), EBRD (9.93%) and Ukrainian Capital Investment Project, which in 2008 bought a stake of 5.97% from Irish AerCap Ireland Limited (formerly Guinness Peat Aviation). The new owners of the UIA are the Capital Investment Project and the Cyprus-based Ontobet Promotions Limited, which they associate with businessman Igor Kolomoisky. After privatization, Aaron Mayberg becomes Chairman of the UIA Supervisory Board. Now 100% of UIA is privately owned.

The main activity of the airline is the performance of passenger and freight transportation. UIA’s fleet consists of 40 modern aircraft: 2 long-haul Boeing 767-300ER, 4 medium-haul New Generation Boeing 737, 24 medium-haul classical Boeing 737 (including one freighter 737-300SF), 5 medium-haul Embraer-190 and 2 Embraer-195E.

The most important priority for the UIA today is safety standards that must correspond and meet high international standards. UIA were the first airline on the territory of CIS countries that received a certificate IOSA (International Operational Safety Audit) and became an international registry as IATA (International Association of air transport).

In 2011, the airline has once again successfully passed inspection for compliance with the requirements of modern operational safety and received their next fourth "certificate" as a reliable provider of IOSA. In May 2014 it is entered into force new requirements for regulation EU 452/2014 for the authorization procedures and security monitoring of aircrafts of operators from third countries (Third Country Operators) that are flying into European airports. A single certificate Third Country Operators authorization replaces all previously issued documents by every European country for UIA and allows airline to fly in the airspace of the European Union and the four countries of the European Free Trade Association - Iceland, Liechtenstein, Norway and Switzerland. This event was followed by another confirmation of the UIA's high level of aviation safety and adherence to operational, which fully meet international ones.

Therefore UIA can be described as:

- Airline actually acts as a monopolist on Ukrainian market by offering the largest number of European destinations from Ukraine than any other airline;
- A modern air carrier that has its network, which enables to connect major cities in Ukraine, and Ukraine with all major cities in Europe, CIS, Asia, the Arab Gulf and the US;
- Reliable airline, which is continually expanding its geography, thanks to agreements with leading aviation companies from all over the world.

Activity of the "Ukraine International Airlines" at the Kyiv Boryspil International Airport

Kyiv Boryspil International Airport (IATA: KBP, ICAO: UKBB) is an international airport in Boryspil, 29 km (18 mi) east of Kyiv. It is the country's largest airport, serving 65% of its passenger air traffic, including all its intercontinental flights and a majority of international flights. It is one of two passenger airports that serve Kyiv

along with the smaller Zhulyany Airport. Boryspil International Airport is a member of Airports Council International. Boryspil airport is equipped with two runways, with the terminals occupying a centre-field location.

Kyiv Boryspil International Airport is the home airport for Ukraine International Airlines. Ukraine International Airlines (UIA) operates all its international scheduled flights, domestic scheduled flights and charter flights to/from Airport's TERMINAL D.

Terminal D area comprises 107,000 m2. Terminal D handles approximately 10 million passengers annually, 3000 pax/h for arrival and 3000 pax/h for departure.

Check-in areas of Terminal D passenger complex has 60 check-in counters and 6 Self-Service Check-in Kiosks, 18 aviation security points, 28 passport control desks which enables passengers to reduce queues. For passengers' convenience there are lifts, elevators and moving walkways.

2.1.1. Production activity of UIA analysis

Ukraine International Airlines (UIA) is Ukraine's leading airline established in 1992. Today, UIA is a 100% privately-owned company and its primary business is to provide safe and reliable passenger and cargo transportation.

Safety is an absolute priority for UIA. Ukraine International was the first airline in the CIS to have earned the distinction of receiving the IATA Operational Safety Audit (IOSA) Certificate, having entered into the IOSA Registry. The IOSA program is an internationally recognized and accepted evaluation system designed to assess the operational management and control systems of an airline. In 2017, UIA has once again successfully completed the IOSA audit. Following the results of International Air Transport Association (IATA) follow-up audit for the compliance with global operational safety standards, Ukraine International Airlines received the seventh IOSA Certificate valid through to June 17, 2019. The IOSA audit covers all aspects of an airline's operations affecting flight safety, including maintenance and flight operation, ground handling, cargo transportation, aviation safety, and company management. UIA today develops new approaches to directions of its business activity.

UIA is a modern network airline with domestic and international operations, connecting Ukraine to dozens of capital cities and key hubs in Europe, USA, the CIS, Asia, and the Middle East.

UIA steadily broadens the geographical scope of its operations, particularly through numerous interline agreements with leading international airlines worldwide. Today UIA operates flights from Ukraine to more than 80 capital cities and key cities in Europe, Asia, America, the Middle East, and the CIS, the carrier performs more than 1100 regular flights per week from Kyiv, Odesa, Lviv, Dnipro, Kharkiv, Zaporizhia, Vinnytsia, Ivano-Frankivsk, and Chernivtsi, offering convenient connections across the globe at competitive prices.

Tickets to any UIA flight are available in different countries of the world in their ticket and representative offices, through a network of travel operators and agencies, as well as on official website, www.flyuia.com, allowing passengers to book tickets online and save time and money.

UIA is a customer-oriented airline offering a flexible pricing policy, convenient flights schedule, a variety of benefits for its Panorama Club Frequent Flyer Programme members, high international service standards and traditional Ukrainian hospitality.

UIA transports various cargo types on all its scheduled flights, as well as on its cargo Boeing 737-300SF aircraft. In order to cover every customers' need, UIA introduced a complete portfolio of cargo services including the following six solutions: Time Definite, Sensitive, Fresh, Live, Valuable and Economic [38].

In comparison with the year prior to 2013 the passenger transportation volume significantly increased. Such changes in passengers' transportation amount we can explain in a such way, in 2013 due to the demise of competitor Aerosvit, UAI launched new flights from Ukraine to Baku in Azerbaijan, Yerevan in Armenia, Larnaca in Cyprus, Munich in Germany, Warsaw in Poland, Vilnius in Lithuania, Prague in Republic, Athens in Greece, Batumi in Georgia, Moscow (Sheremetyevo Airport), Yekaterinburg, Saint Petersburg, Kaliningrad, Novosibirsk, Rostov-on-Don, and Sochi in Russia, Bishkek in Kyrgyztan, and in the beginning of 2014, to New York City in the United States.

As shown in the table 2.1 there was decline of rates in 2014. Reasons of such changes listed below.

Negative factors that influenced on the amount passengers transportation are:

1. In 2014 UIA lost market of Crimea and Donbas.
2. Since August 2014 UIA: fligts around Russia, carries huge direct losses due to excessive fuel consumption, longer runs, a long time in the air, as well as losing the competitive advantages routes through Kyiv, in comparison with the routes that other carriers can afford to lay in the airspace of the Russian Federation.
3. At the end of 2015 added a flight ban in Russia. This is a significant number of flights, passengers that today UIA lost.

In the Table 2.1 amount of passengers by month is represented. The data for 2019 has been taken as an estimate on the basis of data for previous years and information on the official UIA website. In the first half of 2019, UIA has carried more than 3.8 million passengers, the airline said. This is almost 8% more than in the same period of 2018. At the same time, on the regular flights, almost half - 49.3% - is the share of transit passengers.

Table 2.1

Amount of passengers by months in 2013-2019

Months	**Estimated year**						
	2013	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**
January	214789	291735	326015	426483	547191	640213	697833
February	158873	231976	252236	303348	425363	497675	542465
March	179846	265041	276188	319587	401092	469278	511513
April	305967	239845	324981	362814	464970	544015	592976
May	334697	274872	375732	489686	595493	696727	759432
June	503437	365675	509605	616793	693267	811122	884123
July	584627	392457	566074	656497	758636	887604	967488
August	571456	403265	559214	649753	753942	882112	961502
September	517468	378423	482935	604479	678724	794107	865577
October	321457	271942	362938	488536	519658	608000	662720
November	313479	269653	339863	475345	502536	587967	640884
December	426097	334232	385237	554579	595893	697195	759942
Total	4432193	3719116	4761018	5947900	6936765	8116015	8846456

In comparison with the 2018, 2019 characterized by significant growth of passenger transportation volumes. Increasong economic stabilization gave the company possibility to bring a new challenge – to stabilize business in the age of profound political and economic crisis and dramatic decline in effective demand. For the first time ever, company had to take drastic contingency measures and optimize its staff, fleet, and route network. However, national currency has been stabilized lately.

For further business sustaining, UIA modified its operating model and started lowering fares by excluding additional services from the ticket price, thus turning into the world`s first network low-fare carrier. As, it was investigated that, almost most of the airline customers interested in the price policy and only than prefer to choose additional services that depend on the flight reasons.

During 2016 and 2017 years the company actively engaged in route map development enhanced flight geography up to ten Ukrainian cities, launched several new medium-haul flights and increased frequencies on a number of Western European routes. Airline introduced the new onboard menu, and updated a number of web services. However, the landmark of the 2016 is the cut over to Amadeus Altea Passenger Service System, which enables UIA to offer passengers a vast selection of additional services. As a result, company introduced the new check-in concept, and offered low-cost ticket fares.

The most impact on the passenger flow volume in 2016-2018 was caused by active implementation of UIA new strategy – manifesting itself as budget network airline, which was embodied through series of promotions and new conditions for passengers buying tickets in advance. More progressively, it began to be implemented when European Union approved visa-free travel for Ukrainians and some other countries started simplification of the boarder cross procedure that was significantly affected on the passenger flow volumes. Therefore, through price minimization, company got wider range of the market, thereby increasing the number of directions and flights frequency. By that achieved the main regularity of low-cost – aviation product price minimization, by the expense of aircraft downtime minimization, that can be realize firstly thought the

passenger flows volume increasing and secondly – by minimization of aircraft handling time.

The monthly changes in the passenger transportation amount by months in 2013 – 2019 see fig. 2.1.

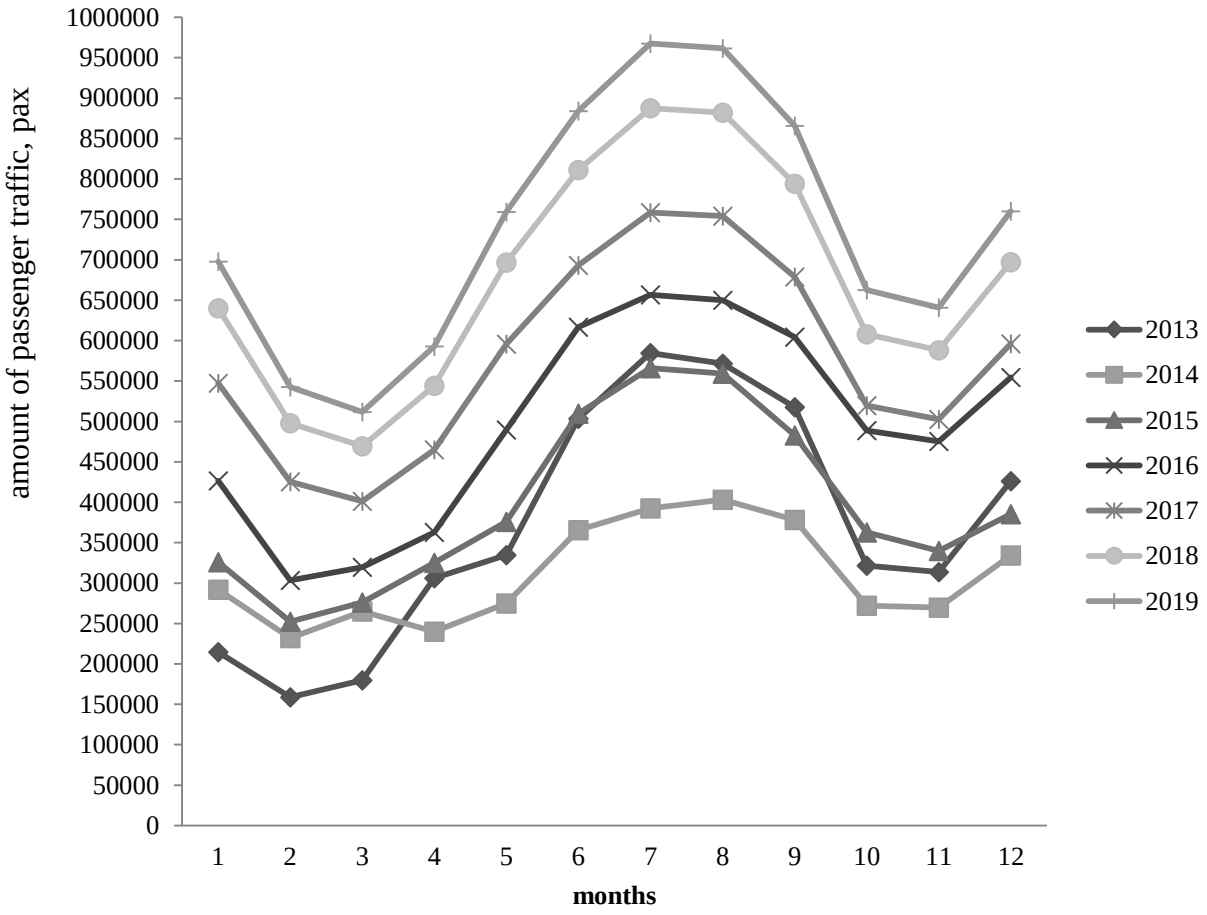

Fig. 2.1. Changes in the passenger transportation amount by months in 2013-2019

Due to the given figure we can more clearly compare variations between seasons. In comparison with previous years in 2019, we cannot observe more smooth transitions between seasons. It means that company strategy gives are not exactly positive results, as it did not start to attract more business travel passengers and tourists, who like to travel between high seasons.

Statistical data (table 2.2) shows us that performance of Ukraine International Airlines within the period of 2013 - 2019 is marked with quality indexes upward trend and figure 2.2 helps us more clearly understand the whole picture of passenger traffic dynamics during the period 2013 – 2019 years.

Table 2.2

Growth of passenger traffic in 2013 - 2019

Indicator	Estimated year						
	2013	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**
Passenger traffic, pax	4432193	3719116	117%	5947900	6936765	8116015	8846456
Growth, %	–	84%	128%	125%	117%	115%	109%

Thus, in comparison with previous year in 2019 UIA increased revenue by 36% - to 685,73mln USD. By the end of 2016, company received a net profit of 14,91 million USD in accordance with International Financial Reporting Standards (IFRS) against a net loss of 19,42 million USD in previous year. In 2015 airline cut net loss in 3,2 times in comparison with 2014, net income increased on 91% - to 772,5 mln USD.

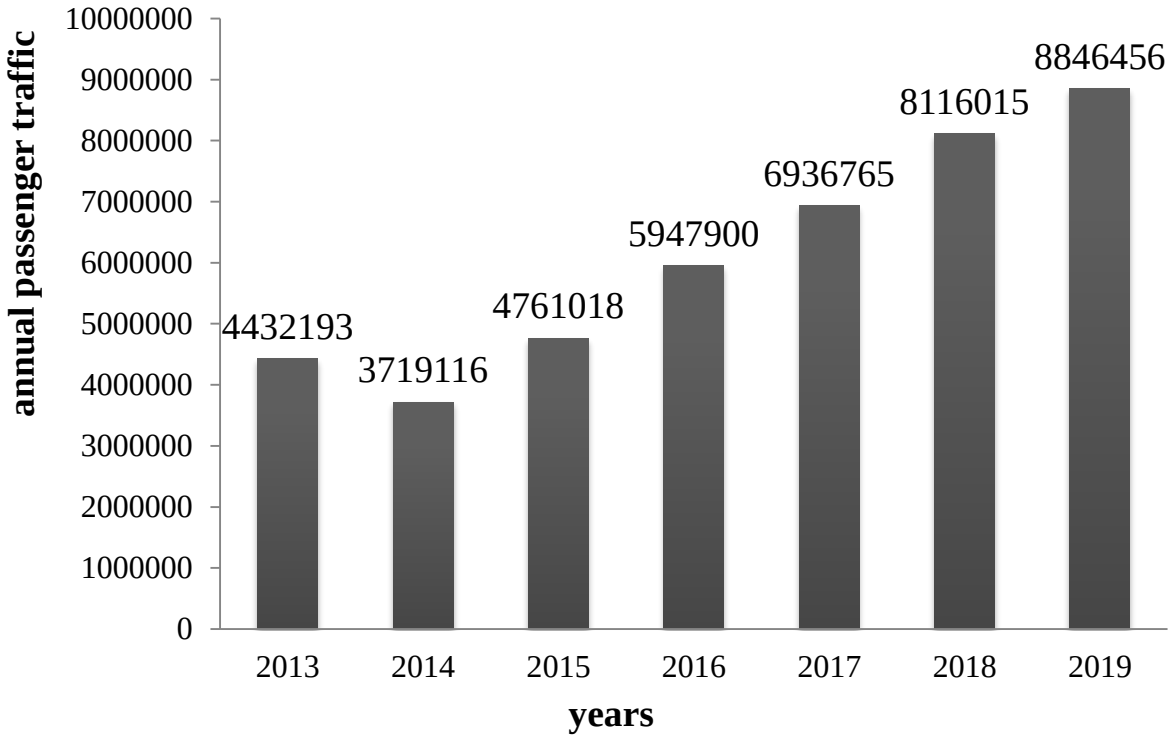

Fig. 2.2. Dynamics of passenger traffic 2013 – 2019

During 2015 year company lost approximately $9 mln because of prohibition of transit through the territory of Russian Federation and ban of direct flights in Russia. The company began to take measures in a way of rescheduling operation in such a way that

the aircraft would not stay idle. 2014 year UIA ends with losses of 113 mln USD, 2013 – with the profit 2,4 million USD.

From the table 2.3 that represented below we can see that starting from 2015 year amount of flights have increased in comparison with 2014 and even higher than in 2013. In 2019, UIA carried more than 8.8 million passengers and, therefore, increased traffic by 9%. The UIA passenger traffic via Kyiv Boryspil International Airport was increased by 18%, up to 7.25 million travelers. Transit traffic on scheduled flights reached 54.1%, domestic transit was increased by 16%, up to 543.4 thousand passengers. International transit was boosted by 22%, up to 2.68 million passengers.

For compensation of losses UIA is looking for new directions: Caucasus, Central Asia, and Near East. When saying that trading with European Union will allow Ukrainian business to replace trading in Russia then for them it is rightly. But for UIA as a carrier for which transit is important only EU few – company needs opposite directions that it can connect through Kyiv.

Table 2.3

Number of flights performed by UIA in 2013-2019, units

Indicator	**Estimated year**						
	2013	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**
I Q	5771	8790	7994	9735	11935	13725	14823
II Q	9720	9051	10543	11850	14026	16130	17420
III Q	13003	11880	12307	14322	15795	18164	19617
IV Q	10063	8495	9983	12829	13192	15171	16385
Total	38557	34816	40827	48736	54948	63190	68245
Growth, %	–	91%	107%	119%	112%	114%	108%

In addition, the carrier improved the occupancy of passenger seats - it increased from 77% in 2018 to 79% in 2019. There is also a positive trend in terms of punctuality of departure of UIA flights - in the first half of this year it was 83% against 77% in 2018. However, the carrier reduced by 0.2% the number of flights to 30 thousand.

In 2015 the carrier launched 19 new non-stop scheduled services – both international and domestic: Kyiv – Beijing; Kyiv – Minsk; Kyiv –Thessaloniki; Kyiv – Amman; Kyiv – Kutaisi; Kyiv – Riga; Kyiv – Zaporizhzhia; Lviv – Odessa; Lviv – Madryd; Lviv – Bologna; Lviv – Rome; Lviv – TelAviv; Odessa– Moscow; Odessa – St. Petersburg; Odessa – Vilnius; Odessa – Kharkov; Odessa – Lvov; Kharkov – Batumi; Kharkov – TelAviv.

Despite of opening new routes, in 2016 – 2017 years UIA continued its development through frequency of flights. Company made more frequent flights: Kyiv – New York – 6 times for a week; Kyiv – Beijing – 5 times for a week, Bangkok in high season – to 5 times a week.

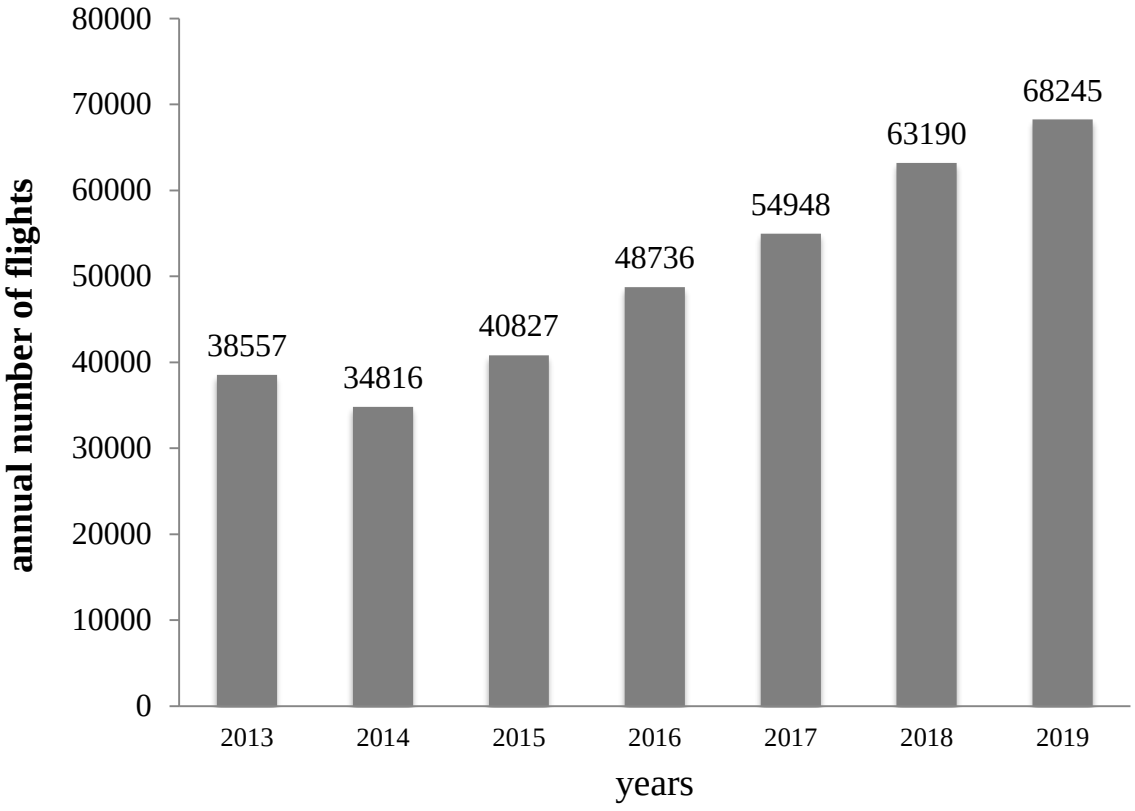

Fig.2.3. Dynamics of flights in 2013 – 2019, units

The airline kept increasing frequencies on the routes between Kiev and Beijing, Colombo, Dusseldorf, Vilnius, Brussels, Madrid, Chernivtsi, and Ivano-Frankivsk, as well as between Ivano-Frankivsk and Alicante. From all flights the most popular are routes: from Kyiv to London, Berlin, Stockholm, Brussels, Paris, Riga, Amsterdam,

Vilnius; from Lviv to Berlin, Paris, Vienna, Amsterdam; from Kharkiv to Srockholm, Riga, Berlin, Vienna,Vilnius; Berlin – Odessa, Chernivtsi – Riga, Amsterdam – Odessa, Amsterdam –Kharkiv. The results of UIA activity concerning flights frequencies grows and new routes opening represented in the figure 2.3.

Regular flights of the airline connect countries of two continents - Eurasia and North America. In Africa, UIA still performs only charter flights. But in April 2018, the airline will fly to Cairo on a regular basis, so the route network will be presented on three continents. Also, in this year company plans to launch non-stop scheduled flights to Toronto (Canada), Eilat (Israel) and Delhi (India), as well as to offer new destinations in China.

Over the course of the following 5 years, UIA expects to expand and renew fleet, actively enhance east and southeast flight vectors, increase frequencies on westbound routes, further develop a hub at Kyiv Boryspil International Airport, and double the number of connecting waves. The latter empowers the carrier to equally distribute operating load and use the existing infrastructure and resources more efficiently.

UIA transports cargo on all its scheduled flights and provides fast and safe carriage of different cargo types: perishable, fragile, valuable, dangerous goods, as well as heavy and oversized freight, diplomatic mail and live animals.

Working partnership with other airlines allows UIA to extend the network to arrange cargo transportation to/from Ukraine to/from any airport worldwide.

The highest result in cargo transportation was in 2013 when the growth rate was fixed on the level of 130 %, whereas the lowest growth was identified in 2014 at the level of 64 %.

During the winter navigation period - from October 1, 2014 to March 29, 2015 – 1226,2 tons of mail and 5040,1 tons of cargo were transported by cargo and passenger flights of UIA, which exceeds the similar figures for the previous winter period by 28,5% and 8,5% respectively. In total, during the winter season 2014/2015, UIA carried 6266,3 tons of commercial cargo.

In the period from January 1 to September 30, 2015, cargo and passenger flights of UIA carried 1,727 tons of mail and 6,997 tons of cargo, which is 9% and 28%,

respectively, compared to January-September 2014. In total, during the reporting period, UIA transported 8,725 tons of commercial cargo.

In 2019, UIA operated 68.2 thousand flights, by 8% more compared to 2018. The average load factor amounted to 80%.

Table 2.4

Amount of cargo and mail transported in 2013 – 2019, tons

Indicator	Estimated year						
	2013	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**
I Q	3398	1326	2862	2953	4145	4642	5060
II Q	3967	2576	3137	3150	3312	3709	4043
III Q	3452	2670	2725	3492	5147	5765	6283
IV Q	4880	3405	3870	4515	5720	6406	6983
Total	15697	9977	12596	14111,2	18325	20524	22371
Growth, %	130%	64%	126%	112%	129%	112%	109%

As seen from the table 2.4, within the period of 2016 -2019 years volumes of cargo transportation have a great positive tendency. One or the reasons of cargo transportation volume growths is singing the agreement between Ukrposhta and UIA about transportation and handling of international parcels and other mail items through Boryspil International Airport using. The project was launched in November 2016 after singing of the relevant agreement. Within the agreement framework were transited about 50 tons of international postal items from China through Boryspil International Airports to countries: Lithuania, Latvia, Armenia, Cyprus and Israel.

In January 2017, mail was transported from the Czech Republic through Kyiv to China. In February 2017, UIA started transportation of its own transit mail from Switzerland to the CIS countries. Such decision will allow in future increase the volume of transit of international postal items through Ukraine, as well as promote the attraction of additional volumes of foreign currency.

Using the data from table 2.4 the graph of dynamics on the quarterly cargo and mail flow of UIA over the estimated period was constructed.

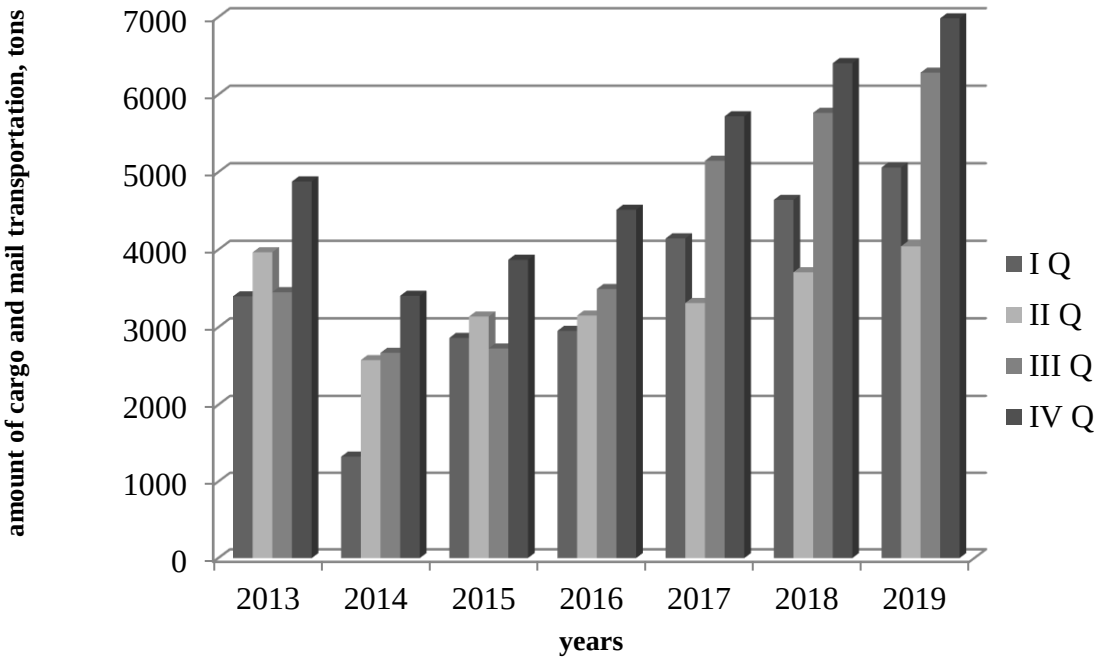

Fig.2.4.Quarterly changes of cargo flows in UIA in 2013-2019

From figure 2.4, the following summary on quarterly fluctuations of UIA cargo and mail flow, specifically the highest rates are observed at the end of the year that can be explained of a large number of holidays that leads to cargo and mail volumes growth.

2.1.2. Financial analysis of UIA activity

All airline receive its profit from aviation activity and non-aviation activity. Aviation activity means passenger and cargo transportation and non-aviation activity includes all additional services that prose airline for example special onboard meal, Interment access, in-flight products, etc.

According to the results of 2012, obtained in accordance with the requirements of the National Accounting Standards of Ukraine “Ukraine International Airlines” for the first time in comparison with previous years reached break-even point and received net profit.

In 2019, the UIA has performed 68249 flights and carried 8,84 mln of passengers that was by 15% higher than in 2018. As evidenced by preliminary financial results of

2018, according to rules of national accounting report of Ukraine, airline profit before taxation reached 10 million UAH.

Despite insignificant profit, receipt of which was the result of extremely hard work of the whole staff of UIA, financial results in 2013 did not allow the airline to fully solve the problem of liquidity and to repay the accumulated losses of previous years.

With the same, positive financial results demonstrate stability of the UIA and tendency to the overcoming of difficult for aviation industry consequences of the global financial crisis.

Main indicators of UIA financial activity are presented in the table 2.5 and dynamics of its changes see figure 2.5.

Table 2.5

Financial indocators of UIA 2013-2018, million USD

Indicator	**Estimated year**					
	2013	**2014**	**2015**	**2016**	**2017**	**2018**
Income	531,5	457,2	587,3	685,7	786,2	910,6
Costs	519,4	455,6	574,5	670,8	770,5	872,2
Operating profit	+12,1	+1,6	+12,8	+14,9	+15,7	+22,7

From statistics of UIA financial activity, we see that from 2015 the income of the company has increased in comparison with previous years. The largest air carrier of the country, in 2015 reduced the net loss by 3.2 times compared to 2014 - up to 504.9 million UAH.

According to the annual report of the air carrier, published in the system of information disclosure of the National Commission on Securities and the Stock Market, its net income in the past year increased by 91% - to 13.133 billion UAH.

In particular increased costs were due to the increased cost of fuel, airport fees and other, advertising costs, increased cost of flight time, the cost of the fleet replenishment. Airline profit increased because of the increased demand on air transportation, increased maintenance services, which contributed to a positive image and attracted new potential passengers to fly with national carriers.

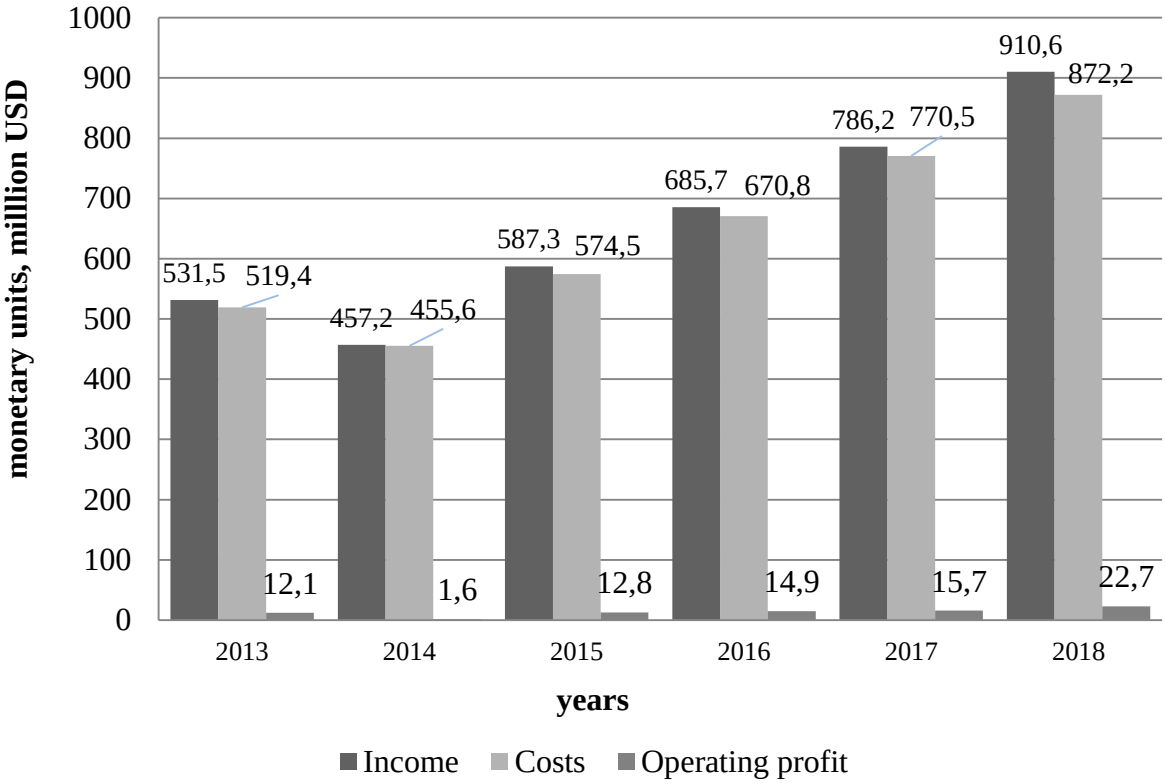

Fig.2.5. Dynamics of airline financial indicators in 2013 – 2018

The main drivers that positively influenced on the income in 2016 – 2017 years are the company poisoning as budget carrier thought range of promotion, additional services improvement, route map expansion and flight frequency growth that are led to the wider consumer market involvement.

Therefore, company implemented range of paid services from which receive additional income:

- ✓ Charge passengers for issuing boarding passes at the check in desk.
- ✓ Introduced payment for the choice of place in advance in the economy class.

Passengers can fix a specific place in the process of buying an air ticket or later through the ticket office at the airport or call center. On medium-haul flights, the choice of any place in the usual row, including the window, in the middle or at the aisle will cost $ 5, in the emergency row - $ 10.

On long-haul flights from Kyiv to the US, China, Thailand, Sri Lanka and in the opposite direction, the usual place will cost $ 10, places in the emergency row - $ 25. The fee is charged for each flight, i.e. if the passenger flies back and forth with a

transfer and wants to pre-select a seat on all flights, he will have to pay a fee for four flights.

As specified in the customer support service of UIA, the passenger will be free to choose a place from available in the process of online registration, which for most flights of the airline opens 48 hours before departure.

For the first time, UIA allowed choosing a place in advance on its flights in April 2015. The service was provided free of charge. The company then said that the future is not going to impose a fee for choosing a location. In the autumn of 2016, after the transfer of UIA from the Gabriel platform to the Amadeus platform, the service ceased to operate and was renewed now for a fee.

Among European airlines, companies such as Lufthansa and KLM take pre-payment for choosing a place. In this case, even in the process of online registration, the choice of free places is very limited.

✓ Internet access service, during the flight, which will be provided on board of the Boeing 777-200ER in 2018. Passengers of business class will receive a free access package with a traffic volume of up to 200 MB. Passengers of premium economy class and economy class will be able to choose one of three access packages for a fee: 20 Mb for $ 7; 50 Mb for $ 15; 100 Mb for $ 23. The traffic between the aircraft and the earth will be exchanged through satellites. The operator of the service will be Panasonic Avionics. To gain access to the Internet, passengers will be able to use any mobile devices with Wi-Fi. Access to the network will be provided after authorization or payment for the service on a special portal.

Aviation market is associated with huge costs. The organization of passenger transportation is no exception. Like any other companies UIA is trying to find ways of decreasing their costs, but with the increase in traffic it is almost impossible. Costs of the company in 2017 are shown in the table 2.6 and on the figure 2.6.

“Operating income” – the common name of the chapter, which records data related to the revenue part of the performed flight: revenue from passenger transportation, mail and baggage. “Non-operating income” – the name of the common chapter, which

records all revenue not related to the flight performance: leasing, receiving of commissions etc. Distribution of UIA costs in 2018 presented in figure 2.5.

Table 2.6

Costs of the company in 2018

Costs	Absolute value, thousand, USD dollars	Percentage value relative to total costs, %
Variable costs	100166	11
Fixed costs	356000	38
Indirect costs	457000	51
Total	910600	100

During its existence the UIA reached all the goals that were set in the foundation documents: creating of international competitive airline with high quality standards, expansion of relations and integration of air transport system of Ukraine in the world aviation network; introduction of advanced technologies and management methods; attracting of foreign investments and getting profit.

UIA became the first airline in Ukraine that received JAR-145 certificate which entitles to perform full maintenance of western manufacturing aircraft. Technical complex of UIA perform maintenance not only of its own fleet, but also of the other airlines fleet in the region.

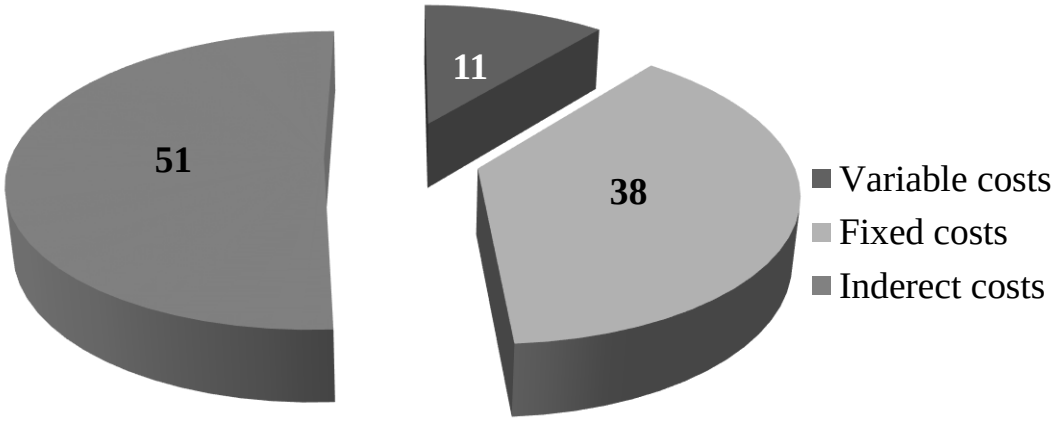

Fig. 2.6. Distribution of costs in UIA in 2018

The main strategic goals of the UIA in the coming year will be:

— developing of the route network and increasing of flight frequency in order to promote development of the company and growth in the number of flights abroad and to Ukraine;

— attracting of new investments and other sources of financing;

— further improvement of the flights quality and customer service;

— increasing of income and revenue;

— leadership in business restructuring of Ukrainian aviation industry.

In the current complicated conditions it is needed to highlight the ways in which the UIA promotes the development of Ukrainian economy:

— attracting of foreign investments;

— avoiding of personnel reduction;

— purchasing of Ukrainian goods and servicing (for example: catering);

— training of the personnel in accordance with the highest international standards;

— world-class management, international accounting standards and business ethics;

— implementing of modern technologies;

— payment of state fees.

2.1.3. Analysis of UIA competitiveness (SWOT)

To identify best practice and critical success factors of total quality management implementation, SWOT analysis was selected to analyze the case of Ukraine International Airlines. The SWOT analysis is the process of analyzing organizations and their environments based on their strengths, weakness, opportunities and threats.

SWOT analysis is an analytical tool used for the identification and categorization of internal and external factors. SWOT analysis can be conducted for a situation, an organization, a project, a new venture, a country, a nation and even individuals. SWOT analysis definition can help organizations in their strategic planning process, and in

matching their capabilities and resources to the competitive environment in which it carries out its operations.

Table 2.9

SWOT analysis of UIA

Strengths	Weakness
❖ leading Ukrainian airline; ❖ developed route network; ❖ ability to segment the market that helps to establish different levels of service and pricing decisions; ❖ affordable price range for Ukrainian with middle-income; ❖ company has its own unique for Ukraine base of full technical and engineering maintenance of Boeing aircraft, which allows providing technical services; ❖ using one type of the aircrafts allows considerably reduce technical maintenance expenses and crew training costs; ❖ full range of technical maintenance ensures; ❖ usage of Amadeus booking system and PROS O&D revenue management system, that interact and help to make market behavior analysis, gives ability to propose new services.	❖ an outdated fleet; lack of comfortable aircraft; ❖ customer expectations of service are increasing; ❖ low competitiveness the under conditions of new low cost carriers appearance on the Ukrainian market;
Opportunities	Threats
❖ explanation of fleet ❖ technological advances can result in the cost savings, from more fuel efficient aircraft to more automated processes on the ground	❖ condition of domestic and global economy; ❖ more successful and dynamic development of competitors; ❖ government operation add to operation costs;

End of Table 2.9

Opportunities	Threats
❖ technology can also result in increased revenue due to customer-friendly service enhancements like in-flight Internet access and other value-added products for which a customer will pay extra; ❖ extend flights to other destinations.	❖ gas and oil fluctuations; ❖ a plague or terrorist attack anywhere in the world can negative affect air travel; ❖ development of rail and maritime network; ❖ low revenues.

While some factors in the SWOT analysis are internal to the venture being undertaken, others are external to it. Internal factors are ones which involve the internal operations and resources of the organization including the strengths and weaknesses inherent to the project/ venture. External factors, on the other hand, are related to the external environment and on which the organization have no influence, including opportunities and threats.

Strengths refer to the internal characteristics, which may be deemed favorable for the organization.

Weaknesses refer to the internal characteristics, which may be deemed unfavorable for the organization.

Opportunities are external characteristics which the organization may use to its advantage.

Threats are external characteristics, which may be potential sources of failure to the organization.

SWOT analysis definition finds applications in a variety of situations and may be applied for assessing the feasibility of the different options available as a solution to a particular problem or challenge. It can also be applied for identifying opportunities and to weigh them against imminent threats and to arrive at a final decision regarding any challenge. SWOT analysis of UIA in table 2.9 helps the company in determining the

factors that will work in their favor and those that will work against them in achieving the desired result and objectives.

Since further in the design part the idea of the given research focuses on the developing of the marketing strategy of UIA we suggest that UIA should consider the analysis of weakness and threats.

2.2. Air transport cybersecurity statistics

It is easy presumed that a possible cyber-attack would have significant social and economic consequences to the air transportation industry. It would also pose a threat to life itself, in case it would result in a plane crushing. Cyber security is considered a significant risk for 85 percent of airline CEOs, regarding the extremely sensitive nature of flight systems and passenger data, based on PwC's 2015 Global Airline CEO Survey [39].

An example of a cyber-attack is the one that happened on June 21, 2015 when LOT Polish Airlines' [39] operations system was hacked resulting in cancellation or delay of 22 flights. It was a Distributed Denial of Service (DDoS) attack on a private network responsible for publishing flight plans.

The data of cybersecurity statistics provided by SITA is analyzed below. The 2018 Air Transport Cybersecurity Insights report is a worldwide study commissioned by SITA. It is the most comprehensive study investigating cybersecurity trends within the air transport industry. The report, that is published by SITA, discusses results from a survey conducted during May to July 2018, which drew responses from 59 senior decision makers at major airlines and airports globally, including CEOs, CIOs, CISOs, VPs and Directors of IT and security practices.

The aim of this aviation-specific research is to determine the state of cybersecurity in the air transport industry and investigate the trends and priorities for investments, current challenges faced by the industry, common initiatives and technology trends, as well as industry-specific risks and best practice.

The 2018 results provide clear insights into the air transport industry's strategic

thinking and plans for cybersecurity in the years ahead. The reaserch also provides expected statictics and data for the year of 2021.

Independent market research agency Circle Research was commissioned to undertake the study on behalf of SITA. The research was conducted in strict confidentiality and the results are presented in an aggregated form only. All source data remains confidential and the results of individual returns are not disclosed to the research stakeholders. A weighting system is applied, based on the respondents' annual passenger traffic statistics, to ensure that the results are a representative sample in relation to global passenger traffic, and to compensate for annual fluctuations in the respondent group.

2.2.1 Analysis of cybersecurity budgets and challenges

The enterprices related to air transportation industry are highly aware of the cybersecurity importance, but the quantity and types of existing challenges are delaying the process of full cybersecurity protection.

Spend on Cybersecurity is increasing in the air transport industry and is set to be higher in 2018 compared to 2017. From the figure 2.7 it can be seen that cybersecurity budgets are growing and spending of the funds is shifting towards detection and prevention, compared to dealing with the consequences of cyber attacks in the previous years.

Airlines spend an average of 7% of their overall IT budget on Cybersecurity, compared to a higher airport investment at 10%. Cybersecurity is not yet getting the investment it deserves, with spend expected to increase to 9% and 12% respectively in 2018. This reflects the rising importance of protecting data and systems from unauthorized access. 73% of respondents ranked regulatory compliance and data privacy regulation as being among the highest priorities. This has been considered an important driver for security investments during the past three years. Security spending is expected to shift towards detection and response in the coming years.

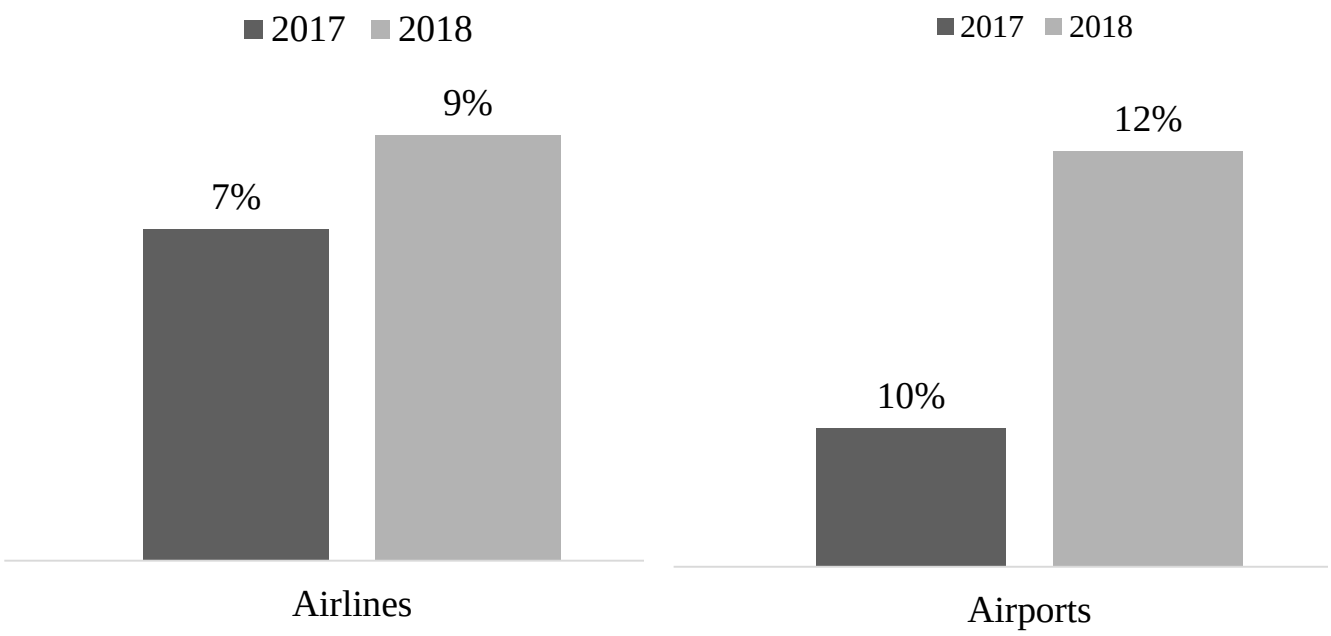

Fig. 2.7 The percentage of IT budget spent on Cybersecurity

It can be seen that security leaders acknowledge the rising risks in cybersecurity, but the teams responsible for cybersecurity are still lacking empowerment and positioning at C-level.

Introducing a dedicated Chief Information Security Officer (CISO) is crucial to visibility and effective implementation. For two thirds of the responding aviation organizations (66%), the overall responsibility for Information Security is assigned to a C-suite executive, reflecting the increasing importance of Cybersecurity to the industry.

Today 41% of respondents include Cybersecurity as part of a global risk register, while a further 42% of respondents planning to include cyber risk in their registers by 2021 (Figure 2.8) . This gives a further indication of the rising stakes in Cybersecurity across the air transport industry.

Yet only 31% of the responding organizations have a dedicated CISO, represented on Figure 2.9. A dedicated CISO can be of pivotal importance for the empowerment and positioning of security teams at C-level.

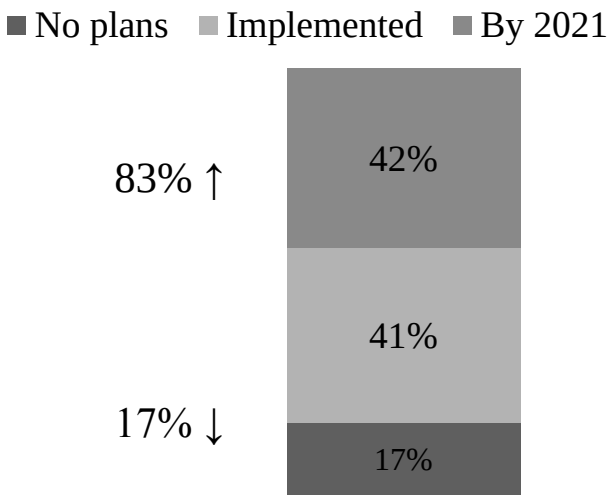

Fig 2.8. The percentage of organizations listing Cybersecurity in their global risk register to improve risk management

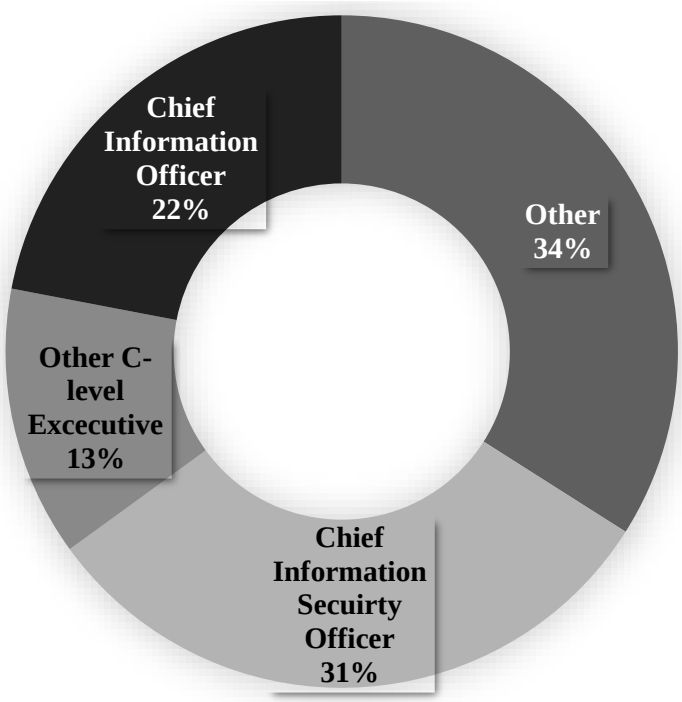

Fig 2.9. Position responsible for Information Security in the organization

Today the majorities of airlines and airports have implemented the core safety mainaining procedures and are ready to advance to the next level. Nowadays 44% of respondents have a formal Information Security Strategy in place (Figure 2.10). By 2021, almost all of the surveyed organizations will have a formal cyber strategy. The most common spending priorities today are: ‘employee awareness and training’ (76%), ‘achieving regulatory compliance’ (73%) and ‘identity & access management’ (63%),

represented on figure 2.11. Regulatory compliance and data privacy regulations have stimulated spending of security during the past three years.

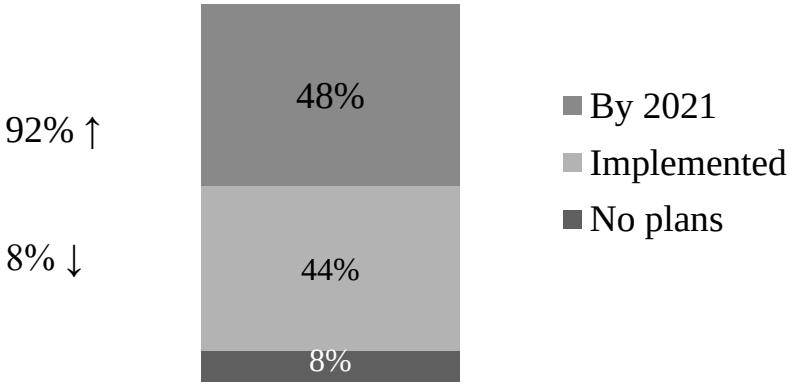

Fig. 2.10. The percentage of organizations with a formal Information Security Strategy

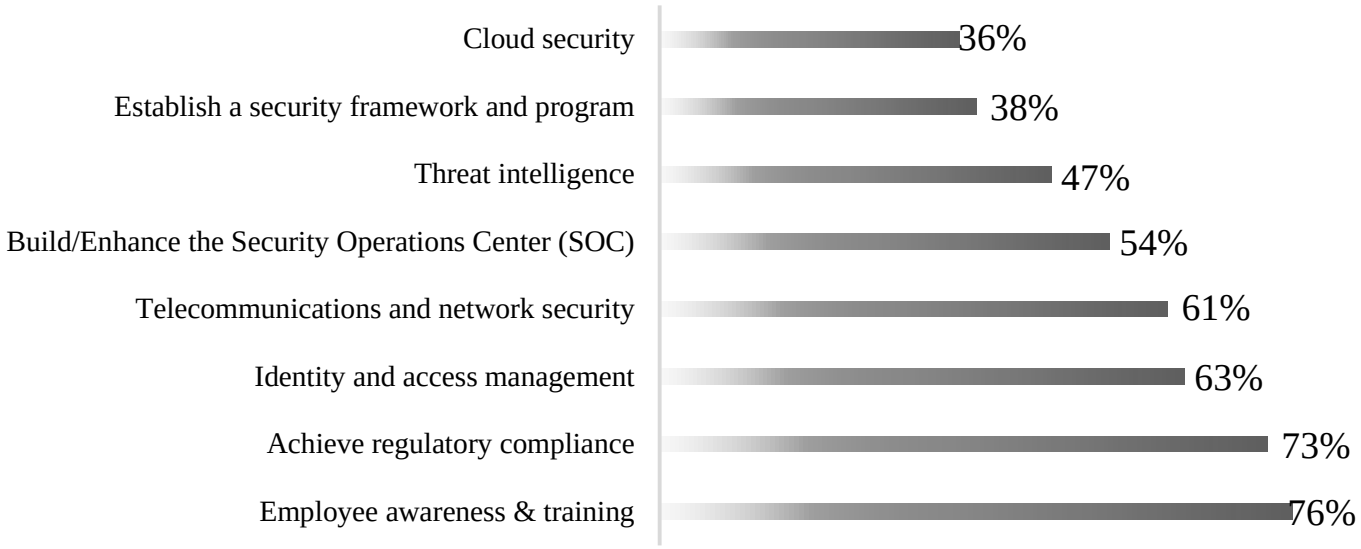

Fig 2.11. Priorities investing in Cybersecurity initiatives

The weakest part of the enterprise regarding the fight against cyber attacks are the employees. Employee awareness is considered the most important component in the defence against cyber risks. Employees are the weakest link in the fight against cyber attacks, and the very first topic to address. Air transport industry security experts accept that employees need to be part of their core security arsenal in the defence against risk. SITA's Air Transport Cybersecurity Insights survey shows that ‘Employee awareness & training‘ is the number one priority for Cybersecurity, represented on the Figure 2.12. With Ransomware and Phishing at the top of the risk agenda, it is good to see such a

high proportion of organizations placing employees at the top of Cybersecurity best practice. Over three quarters (77%) of aviation organizations communicate their security policies to their employees, while 69% have a formal training program in place, data is graphically shown on the figures 2.12 and 2.13.

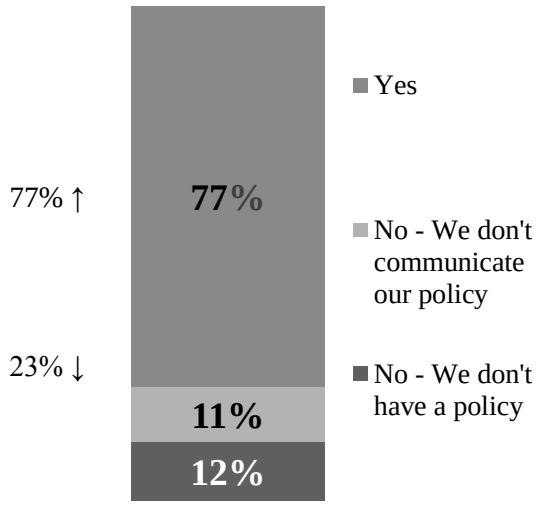

Fig. 2.12. The percentage of respondents who communicate their Security Policies to employees

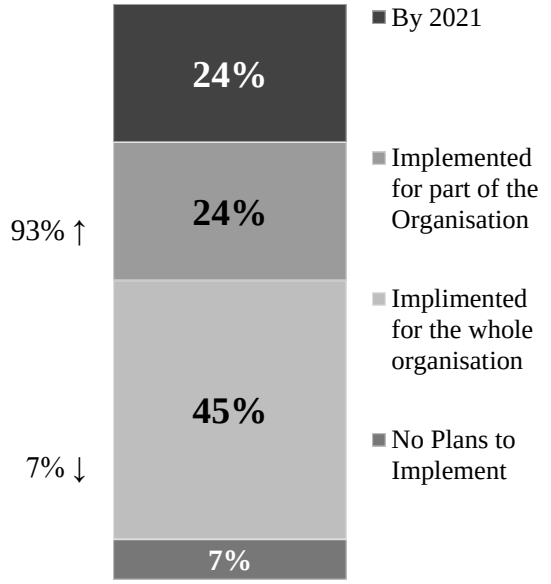

Fig. 2.13. The percentage of respondents with a formal Cybersecurity training program for employees

2.2.2. Cybersecurity statistical data for critical infrastructures

The foundation for an effective cyber security is a formal risk assessment. Securing your organization means being able to assess, detect and appropriately respond to risk and breaches. It is encouraging that the vast majority of the responding organizations are conducting a formal risk assessment today, data represented on figures 2.14 and 2.15. 33% have a Security Operations Center to monitor their IT environment, with another 46% planning to do so by 2021 (Figure 2.16).

Almost two thirds have a defined incident process should a breach occur. Yet, while 73% maintain an inventory of critical infrastructure today, only 40% do the same

for critical business processes. Representation of the data can be seeon on Figure 2.16. This indicates that today the link between business processes and IT systems is missing for many organizations. Linking business process and IT systems enables organizations to manage Cybersecurity based on their potential financial or operational impact.

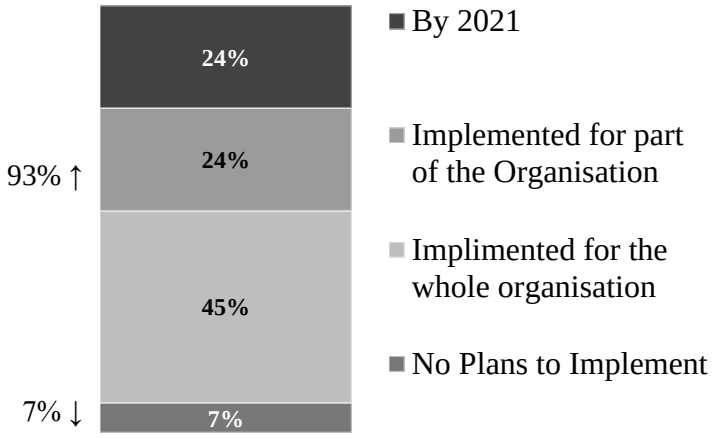

Fig. 2.14. Companies maintaining inventory of critical business processes

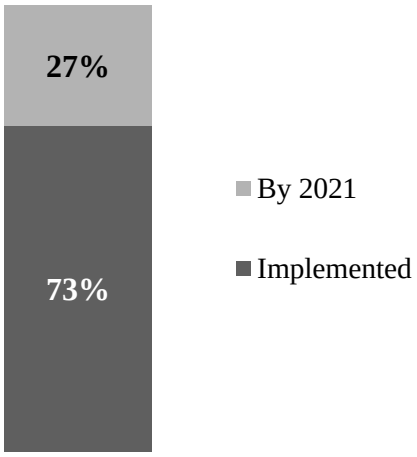

Fig. 2.15. Companies maintaining Inventory of critical infrastructure/applications

Today, proactive protection has become a leading cyber security driver in comparison with compliance in the previous years. What is more, the protaction has a focus on detection external threats and preventing disruption.

Stakeholders state the following top points that should be avoided:

- operational disruptions,

- data loss,
- regulatory fines.

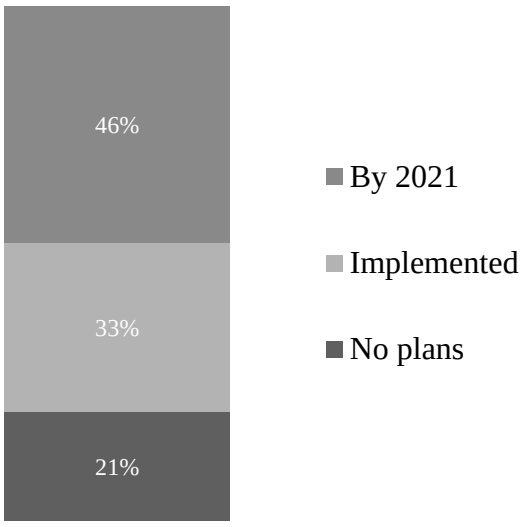

Fig. 2.16. The percentage of companies, which have a Security Operations Center (SOC)

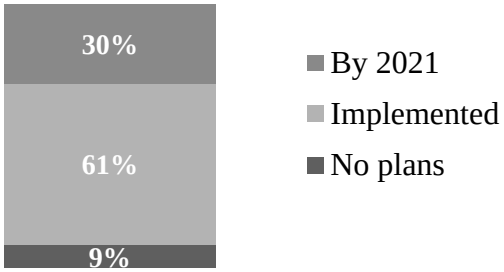

Fig. 2.17. Companies with a defined Cybersecurity incident process

Ensuring business continuity by protecting airport and airline operational processes takes priority in the air transport industry. Industry executives at airlines and airports consider protecting operational systems and processes from cyber attacks to ensure business continuity as their biggest priority overall (Figure 2.18 and 2.19). For airports, disruption is the clear number one concern. Airlines still rank disruption of operations highly (71%) but airline executives also give the protection of their passengers data (78%) and financial loss a similar priority level. The risk of ‘regulatory fines’ is considered a priority for 50% and 42% of airlines and airports respectively. This is likely to increase as the regulatory eco-system globally matures.

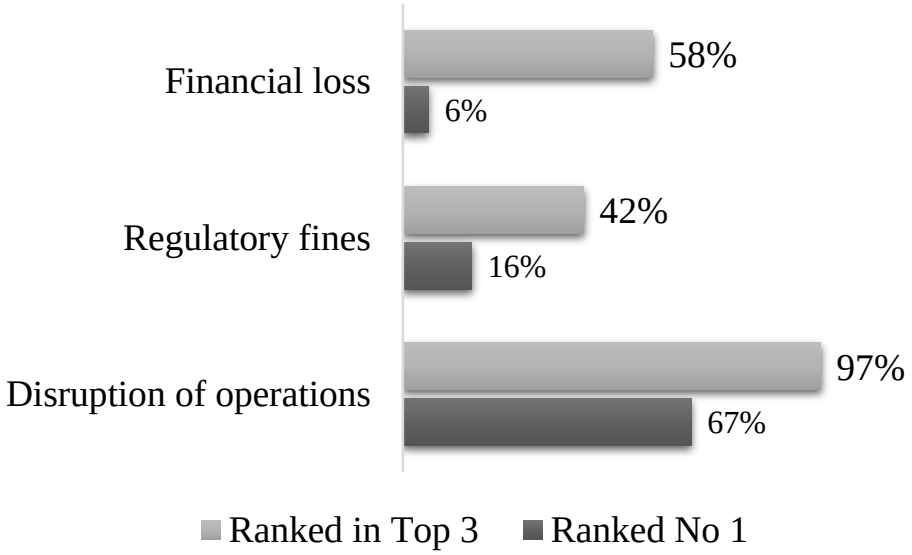

Fig. 2.18. Airports ranking cyber security risks in terms of their priority to prevent

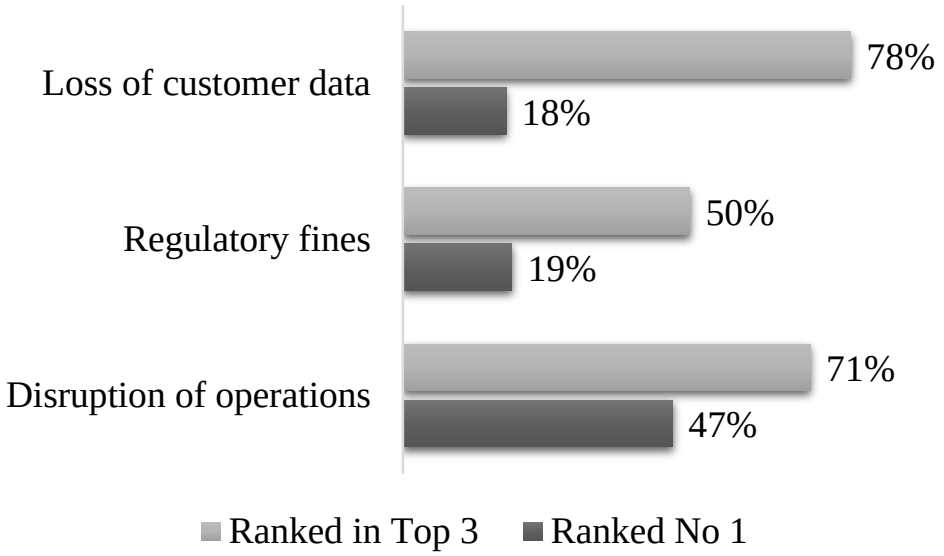

Fig. 2.19. Airlines ranking cyber security risks in terms of their priority to prevent

The analysis of air transport cyber threats is represented in the Figure 2.20 External threats remain the priorities; however there is a consensus that all cyber threats are equally pertinent in the air transport industry. Consistent with other industries, ransomware (58%), phishing (52%) and advanced persistent threats (47%) are regular and frequent risks seen in the air transport industry. Today, more attention is paid towards threats coming from external actors, with only 10% considering insider threats as a top priority today. This area will receive more attention in the future, as analysts

report over a quarter of attacks involving insiders. SITA expects that ‘Shadow IT’ - ranked lower in priority (7%) today - will need to be watched closer in the future. Shadow IT, in particular the adoption of 3rd party cloud solutions by employees, is a trend observed in other industries. It can bring productivity gains but also introduces additional vulnerabilities that need to be carefully managed. Shadow IT, also known as Stealth IT or Client IT or Fake IT, are information technology systems created and used in organizations without the explicit approval of the organization, for example, systems specified and deployed by departments other than the IT department.

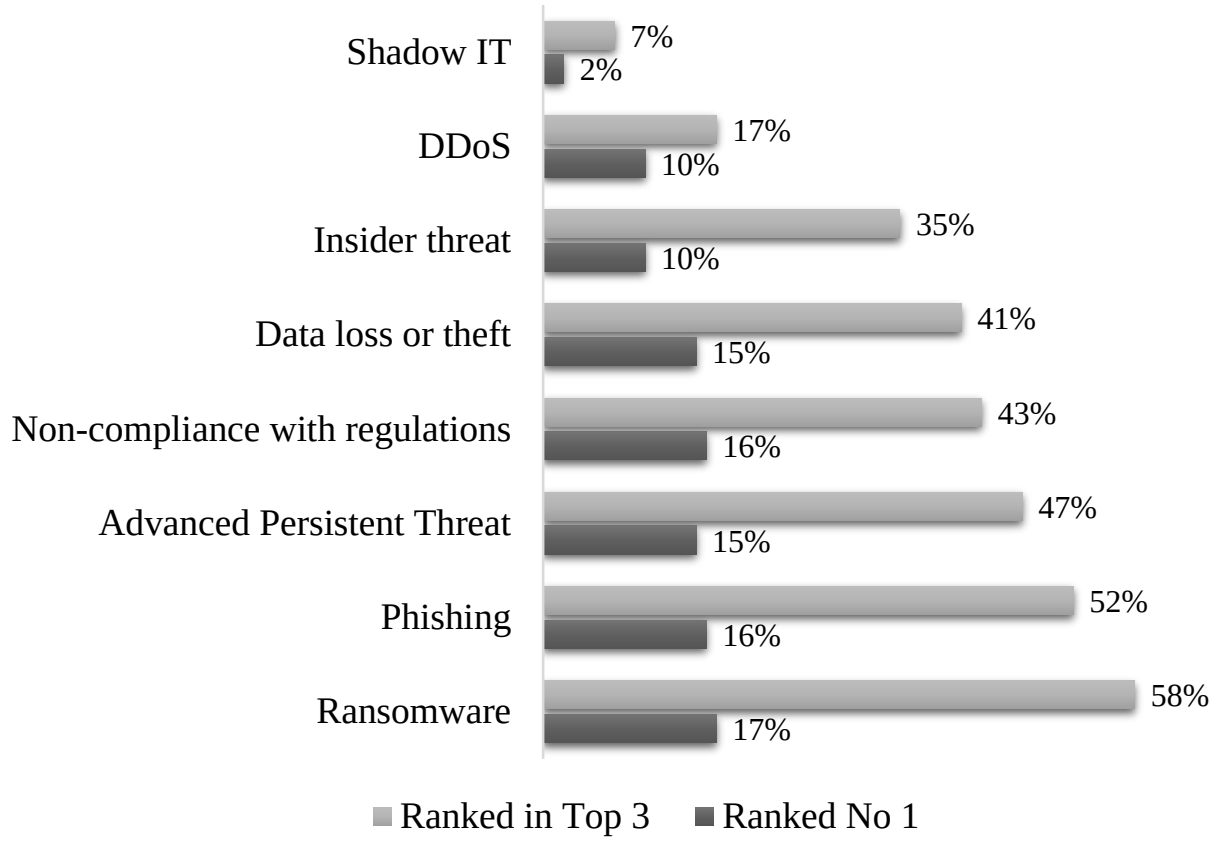

Fig. 2.20. Security risks considered highest priority to address

2.2.3. Analysis in IT security technologies implementation

Core network protection is the priority today. The most common technologies (Figure 2.21) implemented by 2021 will be protecting the edges of the core network, while Internet of Things (IoT) Security, data leakage protection and Cloud access

broker (CASB) will follow as the next technology deployment wave. Deployment of technologies such as CASB, IoT Security and Identity-as-a-Service is limited today. These technologies will see a strong increase in deployment in the next three years as digital transformation progresses and security teams move towards securing the extended enterprise.

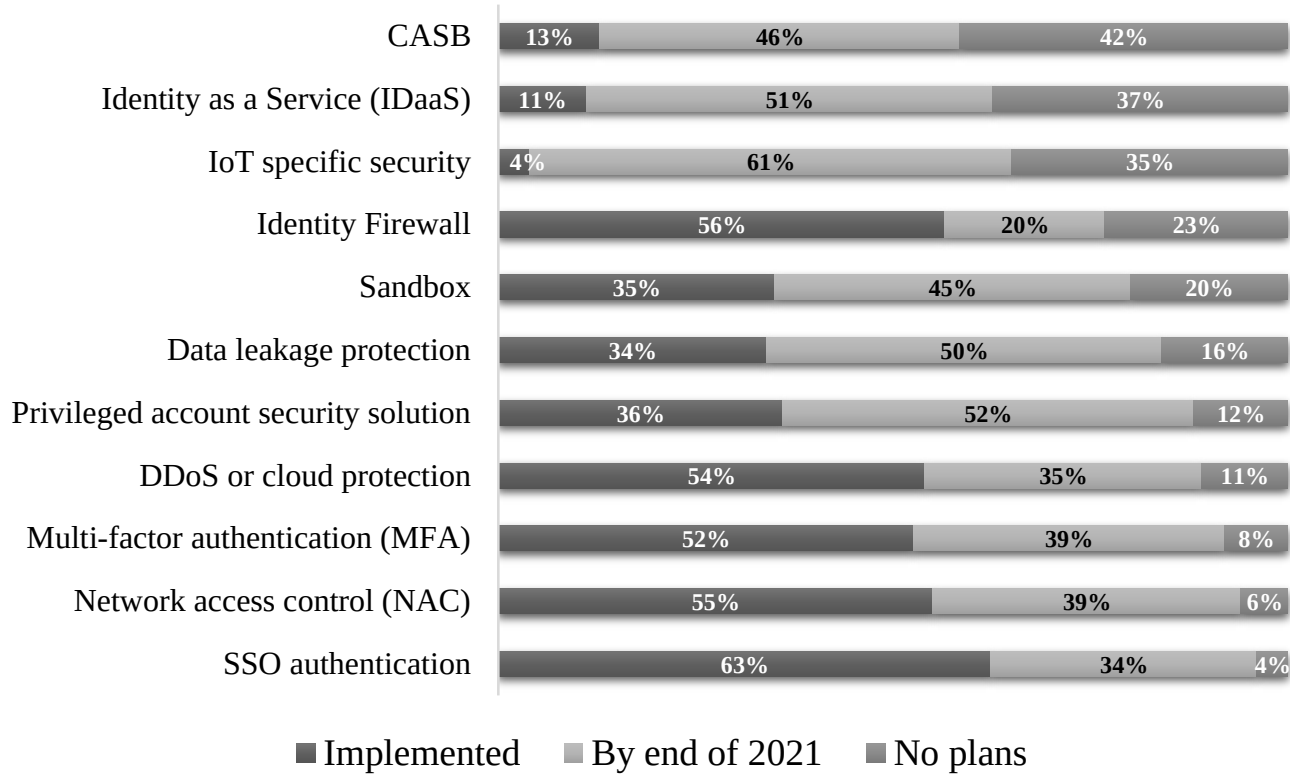

Fig. 2.21. The percentage of respondents with IT security technologies implemented or planning to implement

The immediate objective of ait transportation industry is an implementation os a Security Operations Center (SOC). Proactive monitoring through a SOC is a core topic for proactive Cybersecurity. It is encouraging to see that the majority of respondents have plans to quickly implement such services to enable fast detection of intrusions. A SOC is often the first component security executives look at when building up their cyber defence capabilities. Only 33% of responding organizations have a SOC implemented today, but a further 47% of respondents plan for such investment by 2021 (Figure 2.23). The results also highlight a strong trend towards security outsourcing,

with 8 out of 10 Security Operations Centers today run by external providers (Figure 2.22). Outsourcing SOC services addresses many of the key challenges, in particular, the lack of internal resources & skills which are cited as top challenges implementing Cybersecurity strategy.

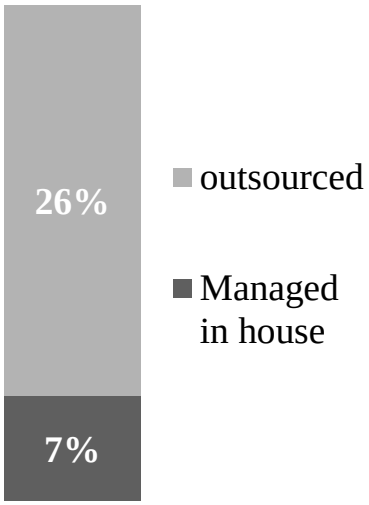

Fig. 2.22. Trends towards outsourcing a Security Operations Center (SOC)

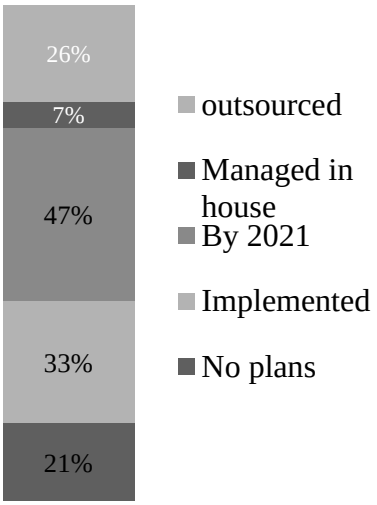

Fig. 2.23. The percentage of those, who have a Security Operations Center (SOC) implemented or plan to implement

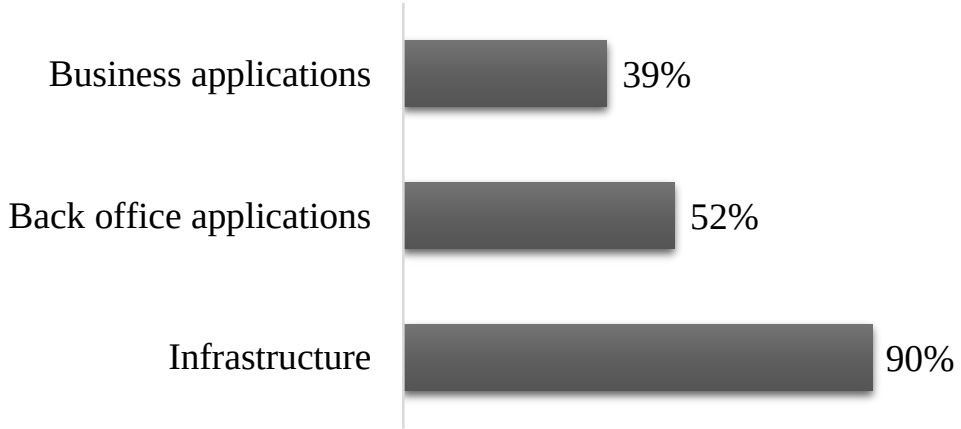

Fig. 2.24. The percentage of network and infrastructure Currently monitored through the Security Operations Center (SOC)

Implementation of SOC emphasizes mostly on the infrastructure level before extending to the application level. Most air transport industry organizations are monitoring their infrastructure through their Security Operations Center today, but have

not yet advanced to the application layer due to the effort required. 9 out of 10 respondents monitor their network and infrastructure through a SOC, while only 52% monitor back office applications and 39% business applications (Figure 2.24). Protecting the infrastructure is quicker to achieve as existing knowledge and best practice already exists. Assessing and monitoring critical applications, in particular bespoke business applications, is more complex than monitoring the infrastructure layer. Monitoring business applications through a SOC requires a deep understanding of how the application behaves and what interactions need to be monitored to detect intrusions. It often needs a high level of effort involving those with in-depth knowledge of the application.

Conclusions to the analytical part

Civil aviation in the context of the globalization of the world economy is an important element of Ukraine's integration into the modern system of international economic relations. Ukrainian International Airline is a major player in the aviation industry of Ukraine. Therefore it has been chosen for the analysis in the master thesis.

The statistics regarding information security and cyber security have been analyzed as well. Data for analysis was taken from a respectful source – SITA. Out of the values and percentages we can make a conclusion that air transport enterprices are highly aware of the importance of cybersecurity, but many existing challenges are delaying process. The growing risk is well acknowledged, but still more must be done to raise the importance of Cybersecurity at both levels – board and at senior management level. The budgets airlines and airport spend on cybersecurity increase year on year and remain in line with other industries. As employees play the most important rule of cybersecurity plans actually working, the most common spending priorities today are ‘employee awareness and training’, achieving ‘regulatory compliance’ and ‘identity & access management’. Further security foundations are being put in place with an objective of continuous improvement. Creating a stronger link between business process and IT systems is key to move towards impact-based protection.

3. DESIGN PART

Air Transportation Management Department				*NAU 20.08.35.300 EN*			
Researcher	*Mariana Y. Khodurska*			*DESIGN PART*	*Letter*	*Sheet*	*Sheets*
Supervisor	*Ivannikova V.Yu.*				*D*	*88*	*40*
Standards Inspector	*Yulia V. Shevchenko*				*FTML 275 ОП-202Ма*		
Head of the Department	*Yun G.M.*						

3.1. Building an Information Security Management System of an airline

Tasks, principles of construction and directions of work for Information Security Management System development:

At each particular enterprise, the construction of an information security system is determined by the following factors [38]:

- financial capabilities of the enterprise;
- technical capabilities of the enterprise;
- the size of the enterprise;
- location of the enterprise;
- nomenclature of products;
- internal document management system;
- the amount of information to be protected;
- type of information to be protected, etc.

The formation of new economic relations between enterprises leads to the problem of the trade secrets mutual protection. In the work practice of foreign firms, the procedure for special agreements on information protection exists and these agreements are transferred to each other in the course of business cooperation.

Tasks of ISMS

Based on the analysis results of possible informational security threats, we can make a list of the main tasks that should be solved:

- control user access to communication channels;
- protection of data transmitted over communication channels;
- registration, collection, storage, processing and issuance of information about all events that occur in the system and related to its security;
- control of the system users by the administration and prompt notification of the security administrator about attempts to unauthorized access to system resources;
- monitoring and maintaining the integrity of protection systems' critical resources and the execution environment of application programs;

- providing a closed environment of proven software in order to protect against the uncontrolled access of potentially dangerous programs and means to overcome the protection system, as well as from the access and spread of computer viruses;
- management of security system facilities.

3.1.1. Basic principles of building an ISMS

The principle of consistency (or systematic approach) requires the need to take into account all the interrelated, interacting and time-varying elements, conditions and factors, that are significant for understanding and solving the security problem. When creating an ISMS, it is necessary to take into account all the weaknesses of the information processing system at the enterprise, as well as the nature, possible objects and directions of attacks on the system by the violators. ISMS should be built taking into account not only all known penetration channels, but also taking into account the emergemce possibility of fundamentally new ways to implement security threats.

The principle of complexity implies the coordinated use of various means in the construction of an integrated information security system, that blocks all significant channels for implementing threats and does not contain weaknesses at the junctions of its individual components.

The principle of protection continuity. Information protection is not a one-time event or a definite set of measures. It is a continuous process involving the adoption of appropriate measures at all stages of information system life cycle, starting from the earliest stages of design but not just at the stage of its operation. Most of the physical and technical means of protection require constant organizational (administrative) support for effective performance, such as timely change and ensuring the correct storage and use of names, passwords, encryption keys, redefinition of authority, etc.

The principle of reasonable sufficiency. It is impossible to create an absolutely safe system. With enough time and money, any defense can be overcomed. Therefore, it makes sense to talk only about some acceptable level of security. It is important to

choose the right level of protection at which costs, risk and the extent of possible damage would be acceptable, which raises the problem of risk analysis.

The principle of management and application flexibility. The measures taken and the established protective equipment, especially in the initial period of their operation, can provide both an excessive and insufficient level of security. To ensure the possibility of changing the level of security, protective equipment must have some flexibility. This property is especially important in cases where the installation of protective equipment must be carried out on a working system without disturbing the process of its normal functioning. In addition, environmental conditions and requirements change over time.

The principle of algorithms and protection mechanisms transparency. The essence of the principle is that protection should not be provided only due to the secrecy of the structural organization and the functioning algorithms of its subsystems. It is extremely important that the knowledge of the protection system algorithms does not make it possible for even the author to overcome it.

The principle of application simplicity. The use of protective equipment should not be associated with the knowledge of special languages or with the implementation of actions that require significant additional labor costs and should not require the user to perform routine operations that are incomprehensible to him.

3.2. ISMS audit standards examination

The audit of IS and / or ITS is performed to meet the requirements of:

- Regulatory documents in the field of technical protection of information of Ukraine (NDI TIC).
- ISO / IEC 27001: 2005
- ISO / IEC 27002: 2013
- PCI DSS.

3.2.1. Comparison of information security approaches ISO 17799 and BSI

Audit of information security management system based on ISO 17799

The ISO / IEC 17799: 2005 International Security Standard is a practical guide to information security. The main goals and objectives of ISO 17799 are: to form a unified, corporate-wide approach to corporate governance systems in the world; structure of general requirements of IB; implementation of IB principles in the organizational structure of companies; developing and implementing an effective security policy.

Advantages of ISO 17799: international recognition; positive perception of business partners; improving the security of the information system; effective information security policy.

Audit of information security management system based on ISO 17799 includes the following:

1. Organizational security measures.
2. Classification and management of resources.
3. Security of personnel.
4. Physical security.
5. Management of communications and processes.
6. Access control.
7. Development and technical support of computer systems.
8. Business Continuity Management.
9. Compliance of the system with the basic requirements.

The German standard for selecting the BSI audit criterion

The standard consists of two main parts: the IB management methodology and components of information technology. In addition, the standard contains directories of security threats and countermeasures (about 600 items in each directory).

Information security management methodology according to BSI:

1. Organization of management in the field of IB.
2. Leadership methodology.

Components of information technology

1. Main components (organizational level of IB, procedural level, organisation of data protection, emergency planning).
2. Infrastructure (buildings, premises, cable networks, organisation of remote access).
3. Client components of different types (DOS, Windows, UNIX, mobile components, other types).
4. Networks of various types (point-to-point connections, Novell networks) NetWare, UNIX and Windows networks, heterogeneous networks).
5. Elements of data transmission systems (e-mail, modems, firewalls, etc.).
6. Telecommunications (faxes, answering machines, integrated systems based on ISDN, other telecommunication systems).
7. Standard software.
8. Databases.

Catalog of Security Threats (Threats and Countermeasures) by Class:

1. Force majeure;
2. Disadvantages of organizational measures;
3. Human errors;
4. Technical faults;
5. Deliberate actions.
6. Improvement of infrastructure;
7. Administrative countermeasures;
8. Procedural counter measures;
9. Software and technical countermeasures;
10. Reducing the vulnerability of communications;
11. Emergency planning.

The International Standard ISO 17799 declares some general principles that are proposed to be specified in relation to the information technology under study.

The second part focuses on the certification of the information system for compliance with the standard, that is, a formal procedure that allows to be convinced of

the implementation of the declared principles. The standard's volume is relatively small - less than 120 pages in both parts.

The disadvantage of the standard is the high qualification requirements of the specialists who carry out the verification for compliance with the standard requirements. In addition, it does not sufficiently take into account the specifics of modern distributed systems.

In the German standard, by contrast, many "individual cases" - different elements of information technology - are considered. The volume of the document is very large - several thousand pages and it will undoubtedly grow. This approach has its advantages and disadvantages.

The advantage of BSI is the specificity of the various elements. In particular, much better than the British standard, the features of providing IB in modern networks are considered. Another advantage is the use of a hypertext structure that allows you to make changes quickly and adjust the relationships between parts of the standard. The downside is the inability to grasp the immense. Many elements of modern information technology are presented at the same level of detail. It is inevitably necessary to introduce the "other" section, which in general looks at the less common elements.

3.2.2. Internarional standard for management of ISMS ISO 27001 and implementation for air transportation industry

This standard is intended to provide a model for the development, implementation, operation, monitoring, review, maintenance and improvement of an Information Security Management System (ISMS). The adoption of ISMS should be a strategic decision for the organization. The implementation of ISMS is expected to scale to the needs of the organization, for example, a simple situation requires a simple solution for ISMS.

This standard can be used by internal and external stakeholders to assess compliance. In the air transport industry the stakeholders are very much interested in the

continuity of operation for both airports and airlines. The non-stop work of any enterprise is closely related to security, particularly information security.

The standard consists of 5 main sections: Information Security Management System (ISMS); Duties of company management; Internal audit of ISMS; Inspections of ISMS by company management; Improvement of ISMS.

The process approach to information security management offered by this standard encourages its users to emphasize the importance of:

1) understanding the information security requirements of the organization and the need to develop information security policies and objectives;

2) implementation of controls and their functioning to manage information security risks of the organization in the context of the overall business risks of the organization;

3) monitoring and reviewing the performance and effectiveness of ISMS;

4) continuous improvement based on objective measurement.

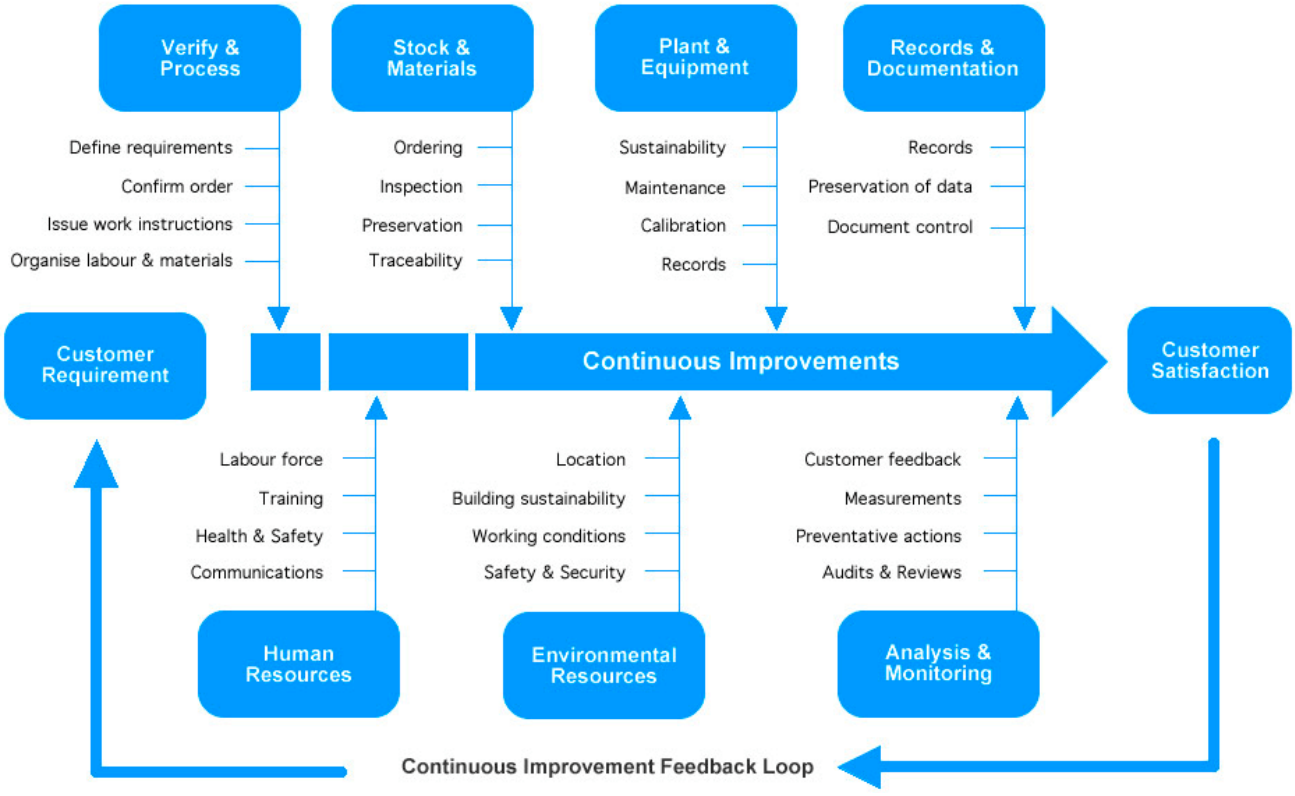

Fig. 3.1 Continuous improvement feedback loop according to ISO 9001

This standard adopts the PlanDo-Check-Act (PDCA) model, which is used to structure all ISMS processes. The standard complies with ISO 9001 (see Figure 3.1)

(quality system development standard) and ISO 14001 (environmental standard) to support the consistent and integrated implementation and operation of an organization's quality system. Thus, one properly designed control system can meet the requirements of all three standards.

3.2.3. Plan-Do-Check-Act model application for an airline

Plan Do Check Act (PDCA) is a very simple, but remarkable process for driving improvement in the design of aviation SMS, and particularly Information Security Management System. PDCA is a cycle and is designed to be repeatable; this feature is represented on Figure 3.2.

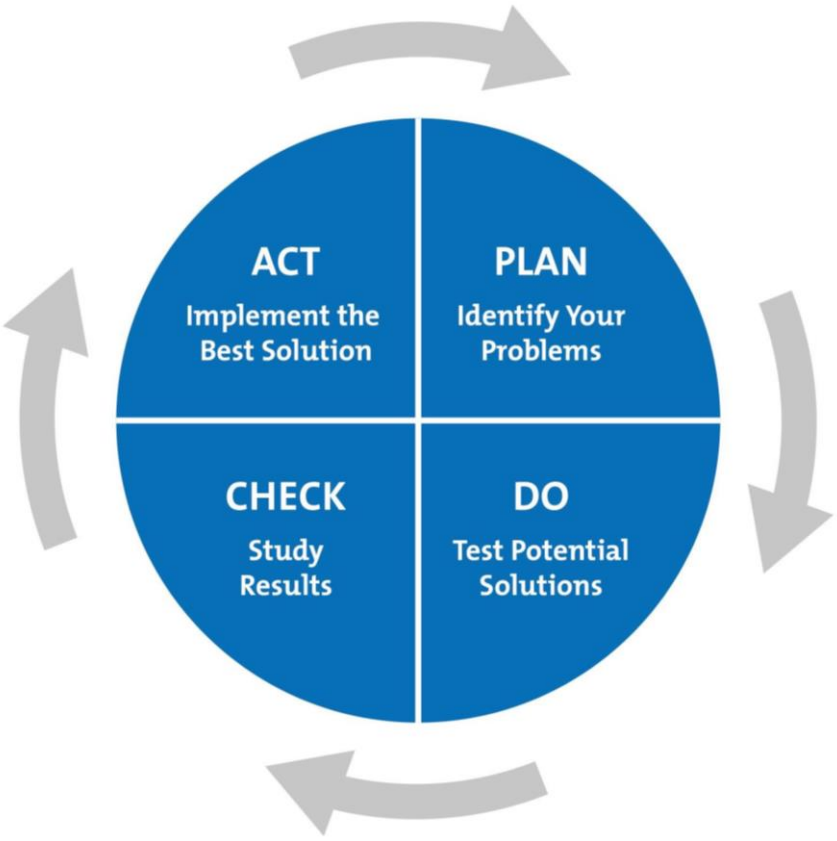

Fig. 3.2. The Plan-Do-Check-Act Cycle

PDCA is most commonly used in the process of creating corrective-preventative actions. It is important to note, that information security audit contains the measures of current IS situation analysis and represents the ways to prevent IS issues in the future.

The acronym PDCA represents the following:

- **Plan**: define what the weakness is, including root causes, and identify how to fix these root causes;
- **Do:** implement the changes that will improve your SMS through assigning corrective preventative actions (CPA);
- **Check:** review the changes to see that they actually correct the weakness as intended; and
- **Act:** make the changes "official" in the organization by updating your operational risk profile.

The phases of PDCA model and points for every step implementation are represented on the Figure 3.3.

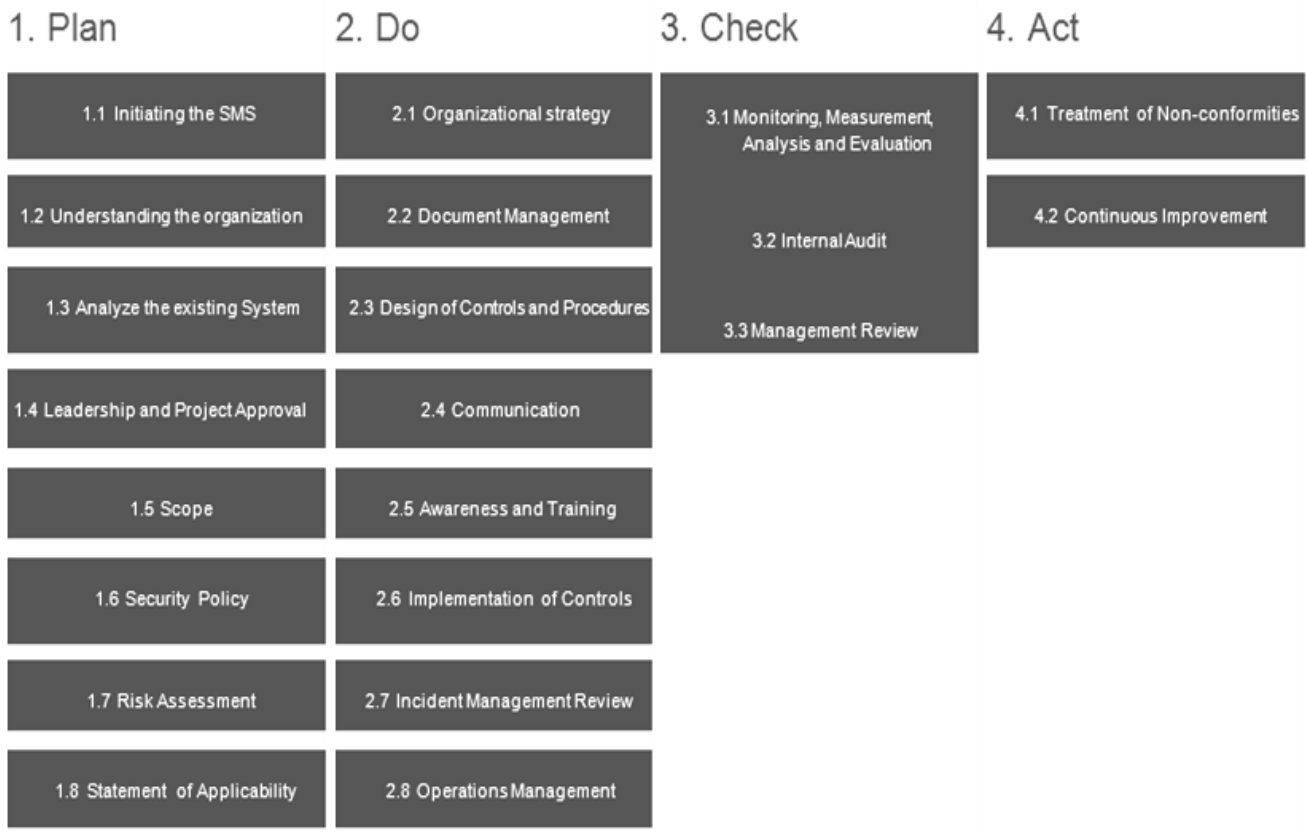

Fig. 3.3. Steps for application of PDCA model

The first phase of PDCA is planning. Safety managers and/or subject matter experts are responsible for this phase, which involves:

- Identifying a weakness (discovery);
- Understanding the root causes of this weakness;
- Identifying how you can fix this weakness by addressing the root causes; and
- Creating a roadmap for fixing the weakness.

Once you have identified the weakness and understand the root causes, you need to outline how you fix the weakness with corrective actions. At a minimum, this "plan" should be a short paragraph that includes: what the corrective action is; the steps that will taken to fulfill the CPA; who will be responsible for carrying out the CPA – i.e., who is assigned the CPA.

"Do" is the second step in the PDCA process. This is the part of the process where the CPA assignee will carrying out the actions to fix the problem. This phase simply includes:

- the subject matter expert who created, assigned, and is responsible for reviewing performance;
- the person who was assigned the CPA and is responsible for carrying out the CPA tasks.

As far as actual responsibility in the Do phase of PDCA, the person assigned the CPA is responsible for "doing" it. In complex environments or with complex CPAs, it's a good idea to perform a safety case on the change and ensure that it is likely to actually fix the problem [41].

The third phase of PDCA is Check, where the subject matter expert who assigned the CPA is responsible for checking to make sure that the CPA performance satisfies intent. Once the assignee finishes CPA tasks, there are two outcomes:

- Assignee performance satisfies the intent of the CPA; or
- Assignee performance does NOT satisfy the intent of the CPA.

Performance can be deficient because the assignee was lax in their duties, in which case you will need to ensure that they repeat the tasks. Performance can also be deficient because the CPA was not planned well (or is the wrong CPA), in which case

you should update your CPA with better tasks or create a new CPA that better fixed the weakness.

A good practice here is to document a performance rating that will be helpful for future review.

Act is the last phase of PDCA and is the responsibility of the Safety Manager to update the System with any changes to the system. In this case, "updating the system" likely means updating your operational risk profile documentation to account for [41]:

- Any risk controls;
- Changes to existing processes, policies, and so on.

Also, you should also strongly consider:

- Communicating any changes to your organization's stakeholders; and
- Ensuring that any changes are incorporated into your SMS review process.

3.3. Implementation of Information Security Audit Department at UIA

The importance of checking information security has been previously discussed in the paper. To check, control and maintain information security a special Information Security Department has to be developed. The structure of the department has to include the following sub-departments represented in Figure 3.4.

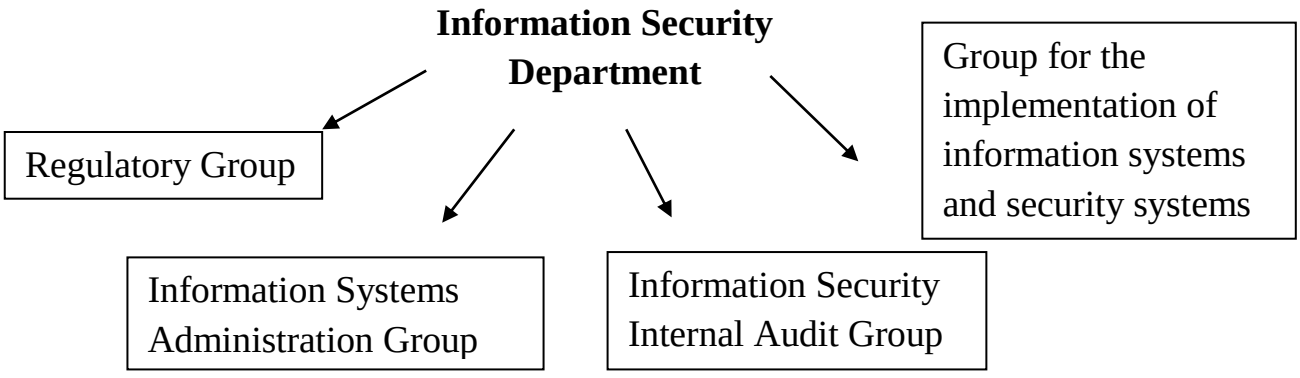

Fig.3.4. The divisions in the Information Security Department

Types of audit are distinguished between external and internal audit.

External audit is usually a one-off event, initiated by management of the organization or shareholders. An external audit is recommended (and is required for some financial institutions and joint stock companies) on a regular basis.

Internal audit is a continuous activity carried out on the basis of a document, commonly known as the Internal Audit Regulations, and in accordance with a plan prepared by the internal audit unit and approved by the organization's management. Information Systems Security Audit is one of the components of IT audit.

We advise to Ukraine International Airlines to conduct and internal audit. There are many cases where it is advisable to conduct a security audit. This is done, in particular, when preparing a technical task for the design and development of an information security system and after implementing a security system to assess its level of effectiveness. The audit is aimed at bringing the current security system in compliance with the requirements of Ukrainian or international legislation. An audit can also be used to systematize and streamline existing information security measures or to investigate an incident involving an information security breach. Usually, external companies providing information security consulting services are involved in the audit.

For the conduction of intermal audit UIA company management has to initiate the auditor. In the cases when audit is outsourced the auditor may be initiated by automation service or information security service. In some cases, the audit is also carried out at the request of insurance companies or regulatory authorities. The safety audit is performed by a team of experts, the size and composition of which depends on the objectives and objectives of the survey, as well as the complexity of the object of assessment.

There are following types of information security audit based on assessment options:

• expert security audit, which identifies deficiencies in the information security system based on the expertise;

• compliance assessment with the recommendations of the international standard ISO 17799, ISO 27001 and ISO 27002, as well as the requirements of the guidelines;

• instrumental analysis of information system security, aimed at identifying and eliminating vulnerabilities of the firmware;

• comprehensive audit, which includes all of the above forms of survey.

Any of these types of audit can be conducted individually or combined, depending on the tasks of the company. The odject of entity can be information system of a company as a whole or its individual segments that process the information that has to be protected.

The main activities in the field of information security audit

The main areas of information security audit are detailed in the following: certification; control of information security; special researches of technical means and design of objects in the protected execution.

Certification of information objects for information security requirements:

- certification of automated systems, communication facilities, information processing and transmission;
- certification of premises intended for confidential negotiations;
- certification of the technical facilities installed in the dedicated premises.

Security control of restricted access information:

- identification of technical channels of information leakage and ways of unauthorized access to it;
- monitoring the effectiveness of the information security measures used.

Special studies of technical means for the presence of electromagnetic radiation and guidance:

- personal computers, communication and information processing facilities;
- local computer systems;
- designing the results of the research in accordance with the requirements of the State Commission.

Designing objects in secure execution:

- development of the concept of information security;

- design of automated systems, communications, processing and transmission of information in a protected execution;
- design of premises intended for confidential negotiations.

The objectives of conducting a security audit are:

- analysis of risks associated with the possibility of security threats against information system resources;

- assessment of the current level of information system security;

- localization of bottlenecks in the information protection system;

- assessment of compliance of IP with existing standards in the field of information security;

- making recommendations on the implementation of new and improving the effectiveness of existing IP security mechanisms.

Incident reports submitted to the Auditor should include documentation of the NIB's so-called "weak points".

Additional tasks facing the internal auditor, in addition to assisting external auditors, may also include:

- developing security policies and other organizational and administrative documents to protect information and participating in their implementation in the work of the organization;

- setting tasks for IT staff related to information security;

- participation in training of information security users and IS staff;

- participation in the analysis of incidents related to information security breach;

- other tasks.

Principles of conducting an ISMS audit

To conduct a high-quality and effective internal audit UIA has to focus on the principles of ISMS audit. These principles should help to make the audit an effective and reliable tool for supporting management policies and management tools, providing information, that an organization can use to improve its performance. Adherence to these principles is a prerequisite for formulating meaningful and sufficient audit

conclusions, and allows auditors who work independently to make similar conclusions in similar circumstances.

We recommend the Ukraine International Airlines to pay attention to the guidelines, which are based on seven principles:

1) Flawlessness: the basis of professionalism. Auditors and those managing the audit program are advised to:

- do their work ethically, honestly and responsibly;
- audit only what he or she is competent for;
- to do their work impartially, that is, to remain fair and impartial in all their actions;
- respond to any interference that may affect their judgment during the audit.

2) Objective representation: the obligation to provide a truthful and accurate report.

The audit findings, conclusions and audit reports must accurately and truthfully reflect the audit progress. Significant difficulties encountered during the audit or any differences of opinion between the audit team and the auditee should be fixed. The exchange of information must be truthful, accurate, objective, timely, clear and complete.

3) Proper professional diligence: diligence and prudence during the audit.

Auditors should exercise due diligence in accordance with the importance of the task they perform and the trust given to them by the audit client and other interested parties. An important factor in performing their work with proper professional diligence is the ability to make informed decisions in any situations that arise during an audit.

4) Privacy: non-disclosure.

Auditors should exercise caution in the use and protection of information obtained in the performance of their duties. Audit information should not be used properly by the auditor or the contracting authority to obtain personal gain or to prejudice the legitimate interests of the audit. This provision also applies to the handling of particularly important and confidential information.

5) Independence: the basis of the impartiality of the audit and the objectivity of the audit findings.

The auditors should be independent and in all cases act in a manner free of prejudice and conflict of interest. In the case of internal audits, the auditors should be independent of the audited functions where possible. Auditors should remain objective throughout the audit process to ensure that the audit findings and conclusions are based only on audit evidence.

In small organizations, internal auditors may not always be fully independent of the audited activity, but every effort should be made to eliminate bias and maintain objectivity.

6) Evidence-based approach: A sound method of obtaining reliable and reproducible audit findings during a systematic audit process should be verified. As a rule, they are based on sampling with the available information, since the audit is conducted with limited time and with limited resources. Appropriate sampling methods should be used because this is closely linked to the level of confidence in the audit findings.

7) Risk Oriented Approach: An audit approach that addresses risks and opportunities. The risk-based approach should have a significant impact on planning, conducting audits and reporting to ensure that the audits focus on issues relevant to the audit client and the achievement of the objectives of the audit program.

3.3.1. Stages of the introduction of an information security audit in UIA

Information system security audit work includes a series of sequential steps that are broadly consistent with those of an integrated IT audit of an automated system that includes:

- initiating the audit procedure;
- collecting audit information;
- analysis of audit data;

- making recommendations;
- preparation of the audit report.

At the stage of initiating the audit procedure, the following organizational issues should be addressed:

- the auditor's rights and responsibilities must be clearly defined and documented in his / her job descriptions as well as in the internal (external) audit provision;
- the auditor must prepare and agree with management the audit plan;
- the internal audit provisions should state, in particular, that company employees are required to facilitate and provide the auditor with all information necessary for the audit.

At the stage of initiation of the audit procedure, the limits of the audit should be defined. The plan and boundaries of the audit are discussed at the workshop, which involves auditors, company executives and heads of departments.

The stage of gathering audit information is the most complex and lengthy. This is mainly due to the lack of necessary documentation on the information system and the need for close interaction of the auditor with many officials of the organization.

Competent judgments about the security situation of an information security company can only be made by the auditor, provided that all the necessary input data is available for analysis. The first item of the audit begins with obtaining information about the organizational structure of the IP users and service units. The purpose and principles of IP operation largely determine the existing security risks and requirements for the system. Further, the auditor needs more detailed information about the structure of the IP. This will allow you to understand how security mechanisms are allocated to the structural elements and levels of IP functioning.

The *methods of analyzing the data* used by the auditors are determined by the audit approaches chosen, which may differ significantly.

The first approach, the most complex, is based on risk analysis. Based on the methods of risk analysis, the auditor determines an individual set of security

requirements for the IP under study, taking the utmost account of the features of the IP, its environment and the security threats that exist in the environment.

The second approach, the most practical, is based on the use of information security standards. The standards define a basic set of security requirements for a broad class of IP, which is formed as a result of global practice. Standards can define different sets of security requirements, depending on the level of IP security to be provided, its accessories (business organization or government agency), and destination (finance, industry, communications, etc.). In this case, the auditor is required to correctly identify the set of requirements of the standard to be met.

The third approach, the most effective, involves combining the first two. The basic set of security requirements for IP is defined by the standard. Additional requirements, taking into account to a maximum extent the peculiarities of the information system functioning are formed on the basis of risk analysis.

The recommendations made by the auditor based on the results of the information system analysis are determined by the approach used, the features of the information system being examined, the security situation and the level of detail used in the audit. In any case, the auditor's recommendations should be specific and applicable to the IS, cost-effective, reasoned (supported by the results of the analysis) and sorted by importance. At the same time, measures to ensure the protection of the organizational level almost always take priority over specific software-technical methods of protection. At the same time, one should not expect the auditor as a result of carrying out the audit, issuing a technical project of the information security subsystem, or detailed recommendations on the implementation of specific software and information security tools. This requires a more detailed examination of the specific issues of protection organization, although internal auditors may be most involved in these works.

The audit report is the main result of the audit. Its quality is characterized by the quality of the auditor's work. It must at least contain a description of the audit objectives, the characteristics of the information system under review, an indication of the audit limits and the methods used, the results of the audit data analysis, conclusions to remedy the existing shortcomings and improve the security system.

3.3.2. Establishing requirements for auditors' competency

In order to achieve the results of internal audit, UIA management has to check the auditor’s competency. The credibility of the audit process and the ability to achieve the objectives depend on the competence of those involved in the audits, including the auditors and the heads of the audit teams. Competence needs to be regularly assessed through a process that considers personal qualities and the ability to apply knowledge and skills acquired through education, work experience, auditor training and audit experience. This process should take into account the needs of the audit program and its objectives.

The basic requirements described in ISO / IEC 27007 are mainly based on ISO / IEC 19011 ("Guidelines for auditing management systems"). They are common to auditors of all management systems, regardless of the management object; others are specificial for specific types of management systems. There is no need for each auditor in the group to have the same competence. However, the overall competence of the audit team should be sufficient to achieve the audit objectives.

Auditors should develop, support and enhance their competencies through ongoing professional development and regular participation in audits.

Determination of auditor's competence

When deciding on the auditor's knowledge and skills relevant to the following, the following should be considered:

1) the size, nature, complexity, products, services and processes of the audit;
2) audit methods;
3) the type of management system to be audited;
4) the complexity and processes of the management system to be audited;
5) types and levels of risks and opportunities addressed by the management system;
6) the objectives and scope of the audit program;
7) uncertainty in achieving the audit objectives;
8) other requirements, such as those established by the audit client or other relevant stakeholders, depending on the situation.

Audit team leaders should have the additional knowledge and skills necessary to provide guidance to the audit team.

General knowledge and skills of auditors of management systems

According to ISO / IEC 27007, auditors must have the knowledge and skills in the areas listed below:

a) Audit principles, processes and methods: Knowledge and skills in this area allow the auditor to ensure consistent and systematic auditing;

b) Standards for management systems and other background documents. Knowledge and skills in this field allow the auditor to understand the scope of the audit and apply the audit criteria, and should include the following:

1) standards for management systems or other regulatory or guidance / supporting documents that are used to establish audit criteria and methods;

2) the application of standards for management systems is checked by other organizations;

3) relations and interactions between the processes of the management system (s);

4) understanding the importance and priorities of a standards set or background documents;

5) the application of standards or background documents in different audit situations.

c) Organization and its context: Knowledge and skills in this field allow the auditor to understand the structure, objectives and methods of managing the audit and should include the following:

1) the needs and expectations of relevant stakeholders influencing the management system;

2) type of organization, management structure, size, structure, functions and communication;

3) a general approach to business and management, processes and related terminology, including planning, budgeting and people management;

4) cultural and social aspects of the audit.

d) Relevant legislative, regulatory and other requirements: knowledge and skills in this field allow the auditor to be aware of the requirements for the organization and to

work within those requirements. The knowledge and skills specific to the jurisdiction or activity of the auditee, processes, products and services should include the following:

1) legislative and regulatory requirements and establish them by state agencies;

2) basic legal terminology;

3) the procedure for concluding contracts and contractual obligations.

Overall competence of the audit team leader

UIA should choose an appropriate responsible person out of the available employees or hire another specialist. According to ISO / IEC 27007, in order to facilitate an effective and efficient audit, the audit team leader should have the competence to:

1) planning the audit and assigning audit tasks in accordance with the specific competence of the specific members of the audit team;

2) discussing strategic issues with senior management of the auditee in order to determine whether they consider these issues when assessing risks and opportunities;

3) establishing and maintaining constructive working relationships between members of the audit team;

4) managing the audit process, including:

- effective use of resources during the audit;
- managing uncertainty in achieving audit objectives;
- the health and safety of members of the audit team during the audit, including ensuring that the auditors comply with relevant agreements relating to health and safety issues;
- leadership of audit team members;
- guidance and consultation of trainee auditors;
- preventing and resolving conflicts and issues that may arise during the audit, including, if necessary, those arising in the audit team.

5) the management of the audit team in order to formulate audit conclusions;

6) preparation and final formation of the audit report.

When auditing multiple systems, a member of the audit team should have an understanding of the interaction and synergies between the various management systems.

Audit team leaders must understand the requirements of each of the management systems standards and be aware of the limitations of their competence in each type of management system.

Ways to ensure auditor competence

We advise UIA to use the recommendations given in ISO / IEC 27007. According to the Standard, an auditor can obtain appropriate competence using a combination of the following:

1) successful completion of training programs that cover the general knowledge and skills of the auditor;

2) experience in relevant technical, management or professional positions related to decision making, decision making, problem solving and communication with executives, specialists, colleagues, customers and other relevant stakeholders;

3) education or training and experience in a specific management system and industry that extends overall competence;

4) audit experience gained under the guidance of an auditor competent in the field.

Criteria and methods for evaluating ISMS auditors

To choose a person for the conduction of internal information security audit we can use the criterias and methods of evaluation. The criteria is of a qualitative nature (eg demonstrating desirable personal qualities, knowledge or implementation of training or workplace skills) and quantitative (eg, work experience and length of study in years, number of audits conducted, number of audit training hours). For an easy assessment we have developed a table that covers all the methods. The assessment is carried out using two or more of the methods listed in Table 3.1.

When using Table 3.1, the following should be borne in mind:

1) the methods described are a set of capabilities and do not apply in some situations;

2) the different methods presented may differ in their reliability;

3) a combination of methods should be used to ensure an objective, consistent, unbiased and reliable result.

Table 3.1

Methods of assessing the auditors

Method of assessment	Objectives	Example
Records analysis	Check the auditor's preparation	Analysis of education records, training, work experience, professional qualifications and audit experience
Feedback	Obtain the feedback about previous auditor's projects	Surveys, questionnaires, personal recommendations, reviews, claims, evaluation of results of work, expert evaluation
Interview	Assess your desired personal and communication skills, confirm information and test knowledge, get more information	Personal interviews
Observation	Obtain the desired personality and credibility to provide knowledge and skills	Role-playing games, observations during the audit, actual quality of work
Testing	Assess the desired personal qualities, knowledge, skills and their application	Exams, psychometric testing

The information collected about the auditor should be compared with the criteria. If the auditor envisaged in the audit program does not meet the criteria, additional training should be provided, additional work experience or audit may be given and re-evaluated.

In order to successfully complete a comprehensive ISMS audit, you must invite a competent auditor. The section considered the requirements for the auditor's competence as well as the auditor's assessment methods. The choice of a professional and independent auditor is a very important factor in conducting a comprehensive audit of ISMS. This will allow us to fully assess the shortcomings of the company in the short term and provide guidance on how to remedy those shortcomings. The auditor should appropriately design the audit program and evaluate all risks and resources for its implementation.

3.3.3. Conducting the information security audit

In general, a security audit, regardless of the form of its conduct, consists of four main stages, each of which performs a certain range of work.

In the first stage, a regulation that establishes the composition and order of work is developed together with the customer. The main task of the regulation is to determine the limits within which the survey will be conducted. The regulation avoids mutual claims on audit completion by clearly defining the responsibilities of the parties. Usually, the regulation contains the following basic information:

• list of people for the working groups from the contractor and the client for audit;

• list and location of the contracted entities to be audited;

• list of information to be provided to the contractor;

• list of resources considered as security objects (information, software, physical resources, etc.);

• a model of information security threats, based on which an audit is conducted;

• categories of users who are considered as potential violators;

• the procedure and time of conducting the survey of customer's information system.

In the second stage, in accordance with the agreed regulation, the initial information is collected. Methods of information gathering include interviewing customer staff, completing questionnaires, analyzing organizational and technical documentation provided, using specialized tools.

The third stage involves analyzing the information collected to assess the current level of enterprise information system security. Based on the results of the analysis, recommendations for improving the level of information system security against information security threats are being developed at the fourth stage.

We have developed a Table 3.2, that represents some steps of audit involved in gatering and analyzing information, as well as developing recommendations for enhancing information system security. The quality of a security audit largely depends on the completeness and accuracy of the information obtained in the process of

collecting the raw data. Therefore, it should include the following: organizational and administrative documentation relating to information security issues, information about the information system hardware and software, information about the security features installed in the information system, etc.

Table 3.2

List of data sources required for a security audit

Information type	The composition of the raw data
Organizational and administrative documentation on information security issues	• information system security policy; • guidance documents (orders and instructions) on storage, access and transfer of information; • regulations for users' work with IS resources;
Host hardware information	• a list of servers, workstations and communications equipment installed in the IS; • hardware configurations of servers and workstations;
System software information	• OS that are installed on workstations and servers; • DBMS information installed in the IP;
Application of software information	• a list of general and special purpose application software installed in the IS; • description of the functional problems that are solved by application software;
Information about security features installed in the information system	• manufacturer of information protection means; • configural security settings; • scheme of protection means installation;
Information about information system topology	• a local area network map, including a scheme for distributing servers and workstations by network segments; • types of communication channels used in IP •network protocols used in the IS diagram of IP information flows.

As previously above, the following methods are used to collect the raw data:

1. Interviewing the staff that knows necessary information. Interviews are usually conducted with both technicians and company executives. The list of questions to be discussed during the interview is agreed in advance. Provision of questionnaires on

specific topics, which are completed by the customer's employees independently. In cases where the submitted materials do not fully answer the necessary questions, an additional interview is carried out.

2. Analysis of the organizational and technical documentation used by the customer. The use of specialized software, which allows you to obtain the necessary information about the composition and settings of software and hardware of the enterprise. For example, security scanners can be used to inventory and identify vulnerabilities in network resources. Examples of such systems include the ISS Internet Scanner and Positive Technologies' XSpider.

Assessment of information system security level

After gathering the necessary information, it is analyzed to assess the current level of the system security. The purpose of information risk analysis is to develop a cost-effective and valid information security system. The objectives of the analysis are:

- comprehensive assessment of IP security;
- estimation of the cost of information (potential loss);
- risk assessment (probability of harm);
- development of a comprehensive security system in line with information risk assessments.

Information risk analysis is necessary to: determine the potential harm (risk) to existing types of valuable information, the ratio of risk to the cost of information security, to assess the effectiveness of information security costs. This analysis identifies the information security risks that the company is exposed to. In fact, the risk is an integral assessment of how effectively existing defenses are able to withstand information attacks.

Methods of calculating security risks

We evaluate the security risk according to the description below. There are usually two main groups of methods for calculating security risks:

1) qualitative;

2) quantitative.

Both qualitative and quantitative assessment methods can be used as criteria for assessing the security of information systems. The criteria for conducting an information security audit are established on the basis of generally accepted international standards (for example, international ISO 17799, German BSI, etc.), internal standards of auditing companies and domestic departmental standards.

The first group allows you to set the level of risk by assessing the degree of compliance with a specific set of information security requirements. The sources of such requirements may be:

• regulatory documents of the company related to information security issues (security policy, regulations, orders, orders)

• requirements of current Ukrainian legislation

• recommendations of international standards - ISO 17799, BS 7799 -2, etc.

• recommendations of software and hardware companies -Microsoft, Oracle, Cisco, etc.

The second group of information security risk assessment methods is based on determining the likelihood of attacks and their levels of damage. Information risk is a value that depends on the level of security of the object and is formulated as:

$$RISK = P\ (probability\ of\ realization\ of\ threat) \cdot Cost\ of\ loss$$

The value of the damage is determined by the owner of the information resource, and the probability of an attack is calculated by a team of experts who conduct the audit procedure. Probability in this case is considered as a measure that as a result of the attack the violators achieved their goals and caused damage to the company.

The methods of both groups can use quantitative or qualitative scales to determine the magnitude of information security risk. In the first case, numerical expressions are taken for the risk and all its parameters. For example, when using quantitative scales, the probability of carrying out an attack P can be expressed as a number in the interval [0,1], and the damage from the attack can be given as the monetary equivalent of material losses of the organization in case of successful attack.

When using qualitative scales, numerical values are replaced by equivalent conceptual levels. Each conceptual level in this case will correspond to a certain interval

of the quantitative rating scale. The number of levels may vary depending on the risk assessment techniques used. Tables 3.3 and 3.4 provide examples of qualitative information security risk assessment scales that use five conceptual levels to estimate damage levels and the likelihood of an attack.

Table 3.3

A qualitative scale for assessing the level of damage

№	The level of loss	Description
1	Low	Minor recoverable loss of tangible assets or minor effects on company reputation
2	Moderate	Substantial loss of tangible assets or moderate effects on the reputation of the company
3	Medium severity	Significant loss of tangible assets or significant damage to the company's reputation
4	High	Big loss of tangible assets and great loss of reputation of the company
5	Critical	Critical loss of tangible assets or complete loss of reputation of the company in the market, which makes it impossible for its further activity

Table 3.4

A qualitative scale for assessing the likelihood of an attack

№	The probability of an attack	Description
1	Very low	The attack will almost never take place. Corresponds to the numerical probability interval [0, 0,25]
2	Low	The probability of an attack is quite low. Corresponds to the numerical probability interval [0,25, 0,5]
3	Medium	The probability of an attack is approximately 0.5
4	High	The attack is likely to take place. Corresponds to the numerical probability interval [0.5, 0.75]
5	Very high	The attack will probably be carried out. Corresponds to the numerical probability interval [0.75, 1]

To calculate the level of risk on qualitative indicators, special tables are used, in which the first column sets the conceptual levels of damage, and the first row - the probability of attack. The cells of the table, located at the intersection of the respective rows and columns, contain a level of security risk (Table 3.5). The size of the table depends on the number of conceptual levels of probability of attack and damage.

Table 3.5

Determining the level of information security risk on a qualitative scale

The level of loss	The probability of an attack				
	Very low	Low	Medium	High	Very high
Low	Low risk	Low risk	Low risk	Medium risk	Medium risk
Moderate	Low risk	Low risk	Medium risk	Medium risk	High risk
Medium severity	Low risk	Medium risk	Medium risk	Medium risk	High risk
High	Medium risk	Medium risk	Medium risk	High risk	High risk
Critical	Medium risk	High risk	High risk	High risk	High risk

Statistical methods, expert assessments or elements of decision theory are used in calculating the probability of an attack and the level of potential damage. Statistical methods provide for the analysis of already accumulated data on actual incidents related to breach of information security. Based on the results of such an analysis, assumptions are made about the likelihood of attacks and levels of damage from them in other information systemss. However, statistical methods are not always applicable due to the lack of statistics on previous attacks on IS resources, similar to the one that serves as the object of evaluation [42].

When using the apparatus of expert assessments, the work results of a group of experts competent in the field of information security are analyzed, which, based on their experience, determine quantitative or qualitative levels of risk. Elements of decision theory make it possible to use more sophisticated algorithms for processing the results of a team of experts to calculate the value of security risk. There are specialized software packages that allow you to automate the process of analyzing the source data and calculating the values of risks in the security audit.

3.3.4. Program for audit results management

The results of the audit have to be monitored. According to the project we place another staff member for audit results management. At the last stage of the information security audit, recommendations are being developed to improve the organizational and

technical security of the enterprise. Such recommendations may include different types of actions aimed at minimizing the risks identified.

Reducing risk through additional organizational and technical protections that reduce the likelihood of an attack or reduce the potential for damage. Thus, installing firewalls at the point of connection to the Internet significantly reduces the likelihood of a successful attack on commonly available in the information resources - such as web servers, mail servers, etc.

Avoiding risk by changing the architecture or scheme of the information flow of the information system, which eliminates the conduct of any attack. For example, physically disconnecting information system segment in which sensitive information is processed from the Internet, avoids external attacks on sensitive information.

Changing the nature of risk as a result of taking insurance measures. Examples of changing the nature of risk include the insurance of IP equipment against fire or the insurance of information resources against possible breach of their confidentiality, integrity or accessibility. Currently, a number of Ukrainian companies already offer information risk insurance services.

Acceptance of risk if it is reduced to a level where it no longer poses a risk to the information system

The recommendations are not aimed at eliminating all identified risks, but only at reducing them to an acceptable level. When choosing measures to enhance the level of information system protection, one fundamental limitation is taken into account - the cost of implementing these measures should not exceed the value of protected information resources, as well as the company losses from possible breach of confidentiality, integrity or accessibility of information.

The person chosen by UIA and managing the audit program must ensure that the following steps are taken:

1) an assessment of the achievement of the objectives of each audit within the audit program was carried out;

2) audit reports reviewed and approved in terms of completeness of audit coverage area and achievement of objectives;

3) analysis of the effectiveness of the measures taken on the results of the audit;

4) the audit report is sent to the relevant stakeholders;

5) identified the need for additional audit.

The person managing the audit program should consider, as appropriate informing non-audit parts of the audit results t and best practices; consequences for other processes.

Audit protocol control

The person managing the audit program must ensure that audit records are created and managed to demonstrate the performance of the audit program. Processes must be in place to ensure that any information security and privacy requirements associated with audit records are met. Entries may include the following:

1) records related to the audit program:

- schedule of audits;
- purpose and scope of the audit program;
- records that identify risks and opportunities within the audit program, as well as relevant external and internal factors;
- the results of the analysis of the effectiveness of the audit program;

2) records related to a specific audit:

- audit plans and audit reports;
- objective audit evidence and conclusions;
- non-compliance reports;
- correction reports and corrective actions;
- follow-up reports;

3) records related to the audit team related to the following issues:

- competence and performance evaluation of members of the audit team;
- criteria for forming audit teams and selecting team members;
- maintaining and improving competence [21].

The form and level of detail of the records should demonstrate that the objectives of the audit program have been achieved.

Audit program monitoring

The person managing the audit program must guarantee the assessment of:

1) that the timetable and audit objectives have been met;

2) the work of the members of the audit team, including the head of the audit team and technical experts;

3) the ability of the audit team to implement the audit plan;

4) feedback from auditors of the organization, auditors, technical experts and other relevant parties;

5) the adequacy and adequacy of documented information on the audit process as a whole.

Some factors may indicate that you need to make changes to the audit program. These may include changes to:

1) audit findings;

2) the demonstrated level of efficiency and maturity of the management system;

3) the effectiveness of the audit program;

4) audit areas and audit programs;

5) the audit management system;

6) standards and other requirements that the organization has undertaken to meet;

7) external suppliers;

8) identified conflicts of interest;

9) requirements of the audit client.

The person managing the audit program and the audit client should analyze the audit program to evaluate whether its purpose has been achieved. The lessons learned from the analysis of the audit program should be used as input to continually improve the program.

3.3.5. Development of Information Security Audit Department

The Inofmation Security Audit Department is being developed in this section. We strongly recommend to implement a new separate department that will be dealing only

with the reasons of Information Security and within it, develop an Audit Department. At the current moment, sadly, information security for our country is most often a fashionable thing, with an incomprehensible purpose. For management, this is basically a bottomless hole for financing, from which there is no return, except for the words: everything is under control. Based on this misunderstanding, all the IS problems in organizations and, in fact, the organization of information security itself are emerging.

The most common problem - to whom is information security related? The two main archetypes are submission to the security service (economic, personal, etc.) and IT department. Both of them are not enough to fully cover all information Security tasks, therefore we develop Information Security Department with a group responsivble for Information Security Audit.

In any of these archetypes there is a problem of passive resistance due to the number of matching levels. In the worst case (from my own experience), the coordination vertical looks like this:

- Employee creates document;
- The direct manager agrees;
- The director of the department agrees;
- Agrees Deputy Director General;
- Signed by CEO.

Each of the stages takes some time, and with an increase in the level of coordination, this time grows in progression. As a result, documents can hang for quite some time, the electronic document management system will save the situation, but not 100%.

Ideally, submission directly to the general or first deputy, as an option - deputy for security. The most convenient thing is, of course, the deputy security officer. In this case, you can get the advantages of the first option, while reducing the vertical coordination and decision time.

The purpose of this section is to calculate the cost for developing Information Security Audit Department at UIA. This department will be able to conduct an internal

audit of information and cybersecurity by responsible specialist, compared to the involvement of external private audit firms.

The reasons why we choose the internal audit are the following:

- It is aimed at assessing the company's existing control and risk management systems to effectively achieve the company's goals;
- Serves the interests of the board of directors and managers of the company;
- It is aimed at assessing the economic feasibility of managerial decisions and the performance of company divisions.

The organizational status of the internal audit department. The internal audit department should not be subordinate to the executive bodies of the enterprise. Otherwise, the objectivity of the internal auditor is lost when checking the activities of the persons in whose subordination he/she is. The organizational status should be sufficient to guarantee a wide field of action for internal auditors, an adequate discussion of their proposals and the effectiveness of actions in accordance with the developed recommendations.

Firsly, we make a list of company members that are involved in the audit process. To conduct an internal audit of information and cyber security it is necessary to involve:

- internal information safety specialist;
- information technology specialist;
- manager responsible for information security application and modernization;
- security deputy;
- legal counsel, that is specialized on information security;
- accountant.

We assume that every staff member has a monthly salary – 1000 USD. For further minimization of costs, legal councel and an accountant can be outsourced. The expected monthly pay for 10 working hours per week, in this case, would be 120 USD.

To determine the effectiveness of internal audit program we calculate:

1) The cost of conducting an internal audit of information and cyber security of an airline;

2) probable costs for the audit certification of airline staff;

3) probable capital expenditures for the audit process itself.

In order to increase the efficiency of the safe information functioning of the airline audits of ISMS are conducted. Audit can be carried out by the staff of UIA, by State Enterprise "Ukrainian Special Systems" or a private organization the provides autit services.

From the online sources it can be found that before applying for CISA training course, you should first pass an exam. First, you must register for the CISA exam - Early Registration is $415 for Members and $545 for Non-Members; Final Registration is $465 for Members and $595 for Non-Members. You must then pass the CISA examination and apply for certification.

The certification update is required every 3 years and costs $215.

Certification will only be awarded to candidates who meet the experience requirements. CISA certification requires a minimum of 5 years of professional work experience in information systems auditing, control or security. Substitutes to work experience may be applied for a maximum of 3 of the 5 required years.

The abovementioned certification is very cost-effective for any airline, particularly UIA, as it is a large organization which has a special budget for information security. It is proposed to add certification of appropriate staff memebers to ISMS budget.

The complexity of conducting information and cyber security audits by airline staff is determined by the duration of each work operation, starting with the preparation of the audit program and ending with the documentation (subject to the work of one specialist):

$$t = t_{pi} + t_{ig} + t_{da} + t_r + t_{ar} + t_c \quad (3.1)$$

$$t = 24 + 72 + 64 + 32 + 24 + 80 = 296 \text{ person/hour ;}$$

where t_{pi}=24 – duration of audit procedure initiation, person / hour;

t_{ig} = 72 – duration of information gathering, person / hours;

t_{da} = 64– the duration of the audit data analysis, person / hours;

t_r = 32 - duration of preparing recommendations, people / hours;

t_{ar} =24 – duration of the audit report preparation, person / hours;

t_c = 80– duration of courses, people / hours;

The cost of auditing and cybersecurity by airline staff consists of the cost of the contractor's salary – C_{salary}, the cost of machine time required to process the audit data on the PC $C_{machine\ time}$.

$$C_{auditing} = C_{salary} + C_{machine\ time} \quad (3.2)$$

$$C_{auditing} = 1708\ USD + 15\ USD = 1723\ USD$$

The salary of the contractor takes into account the basic and additional wages, as well as the deduction of a single social contribution (22%) and is determined by the formula:

$$C_{salary} = t * C_{salary\ per\ hour} \quad (3.3)$$

$$C_{salary} = 296 * 5.77 = 1708\ USD$$

where t – total duration of internal audit, hours;

$C_{salary\ per\ hour}$– salary of specialist with accruals, USD / hour,

There are 173.3 working hours a month, so in order to determine salary per hour we devide 1000 USD per 173.3, whick makes 5.77 USD per hour.

The cost of machine time to process the collected information on a PC is determined by the formula:

$$C_{machine\ time} = (t_{pi} + t_d) * C_{machine\ hour} \quad (3.4)$$

$$C_{machine\ time} = (296+3) * 0.05 = 15\ USD$$

where t_{pi}– installing the program on the PC, hours;

t_d – complexity of preparation of documentation on the PC, hours;

$C_{machine\ hour}$ – cost of 1 hour PC time, UAH / hour.

Cost of 1 hour PC time is determined by the formula:

$$C_{machine\ hour} = P * T_{Electricity} + (RV_{PC} * D_a) / WT_{annual} \quad (3.5)$$

де P – installed PC power, kW;

$T_{Electricity}$ – tariff for electricity, UAH / kW * year;

RV_{PC} – residual value of PC for the current year, UAH;

D_a – annual depreciation rate on a PC, unit;

WT_{annual} – annual working time fund (for a 40-hour work week).

An average yearly price for electricity operation PC is 100 USD. There are 2080 working hours a year. So the price for 1 hour PC operatinf is 0.05 USD.

The residual value of a PC is determined based on the actual life of the PC as the difference between the original cost and the wear and tear over time.

It should also be noted that before conducing the first audit, the staff has to complete Security Audit cources. Therefore, the price will increase by 595 USD multiplied by 3 (at least 3 staff members should be certified), which makes 1785 USD. The cost of auditing determined is part of a one-time capital expenditure that can be used in an airline.

The internal audit, according to the project, is conducted once every 3 month. The total cost for the 1st audit year is:

$$TOTAL\ COST = C_{cources} + C_{auditing} * 4 = 1785 + 1723 * 4 = 8677\ USD \quad (3.6)$$

The next years will not include the costs for cources complination, but will include the updates on the certificates.

For the convenience of audit procedure, we have developed a questionnaire that can be used and filled in by the performer of audit. The process and tasks that are completed by the internal audit specialist is described in Table 3.6. The questionnaire can be used by the manager and the performer for monitorinf tht tasks that have already been completed and those, that will be done in the future. The Questionnare, if needed, can also include a column with a link to document, that describes the procedure.

Table 3.6

Audit plan and determining the objectives of its implementation (questionnaire)

Audit start date:		
Audit end date:		
Procedure		Performer
1	Analyze reports on previous checks, including also reports on the control of subsequent corrections; identify and document the measures that need to be taken to correct the deficiencies noted	

End of Table 3.7

2	Compare the time spent during previous audits with the actual results and conclusions of this audit. Based on the results of previous inspections, write down your recommendations (if any) regarding changes in the scope of inspections	
3	Document any changes that may be currently made to the audit risk assessment identified during the previous audit.	
4	Clarify the point of view of independent auditors regarding the existence of significant problems in the department that is planned to be checked, as well as their wishes regarding any special tests by internal auditors	
5	Summarize and document the tasks of the audit in order to focus efforts on the implementation of tasks and facilitate further assessment of their implementation	
6	Prepare an audit schedule	
7	Develop a detailed audit program and approve it with the head of the audit team	
8	Draw up and send a notice of the planned audit, the timing and objectives of its implementation to all who should be aware	
9	Document the reasons for choosing one or another level of management, with whom the results of the audit will be discussed and to which a report will be provided to ensure that the selected level of management has the authority to implement agreed recommendations to solve the problems identified	
10	At a preliminary meeting with the management of the audited department, discuss the audit tasks. Obtain and document comments and suggestions from management regarding ways to facilitate obtaining results during verification	
11	Based on the information obtained at the preliminary meeting and our own research, draw up a detailed audit program and, if necessary, reflect in it the results of meetings with management and our own inspections of the state of affairs in the audited unit	
12	Document changes made to the detailed audit program and approve it with the management of the audit team	
13	To compile a report on amendments to the budget for the purpose of documenting the amendments	

Economic reasoning of internal audit

The economic effect of conducting an internal audit is that the UIA may not use other commercial and government entities to conduct an internal audit of information and cybersecurity at its enterprise.

Costs of internal information security audit will definitely be smaller than costs for external audit. Moreover, the airline will be able to conduct the audit more regularly than use the services of commercial or governmental organizations.

The costs of commercial organization services are always individual and depend on many factors, but there is an approximate pay for information security audit at the enterprise where, the number of employees is more than 2500 people, and the activity is connected with highly technological and sensitive equipment – around 900 thousand – 1 mln UAH or approximately 38 thousand USD.

Conclusions to the design part

Information security audit is one of the most effective tools today for obtaining an independent and objective assessment of the current level of enterprise security against information security threats. In addition, the audit results provide the basis for the formation of a strategy for the development of the information security system of the organization. However, it must be understood that a security audit is not a one-off procedure and should be conducted on a regular basis. Only in this case will the audit bring real value and help to increase the level of information security of the company.

To ensure the effective operation of the system, it is necessary to audit the ISMS, which in turn is based on a number of principles. Only by adhering to them can we reach meaningful and sufficient audit conclusions. In order to properly audit the ISMS, a competent and experienced auditor must be invited.

This section describes the brief recommendations of ISO 17799, ISO 27001, and ISO 27002 for successful audit program development, goal setting, and audit risk assessment. Another important aspect is the analysis of available resources, which will allow you to correctly divide the audit into stages. The audit program must be monitored and recommendations made to improve the audit program. At the conclusion

of the audit, the auditor should submit a report documenting information about the audit process as a whole.

In the design section recommendations for calculation of audit costs have been proposed as well. The calculation includes duration of all processes that are included in the internal information security audit, the cost of auditing and cybersecurity by airline staff and the salary of the contractor that conducts the audit.

SUMMARY

Air Transportation Management Department				*NAU 20.08.35.002 EN*			
Researcher	*Mariana Y. Khodurska*			*SUMMARY*	*Letter*	*Sheet*	*Sheets*
Supervisor	*Ivannikova V.Yu.*				*D*	*129*	*3*
Standards Inspector	*Yulia V. Shevchenko*				*FTML 275 ОП-202Ма*		
Head of the Department	*Yun G.M.*						

In order to assess the real state of security of information and communication systems (ITS) resources and their ability to withstand external and internal security threats, it is necessary to carry out regular audits of information security.

The purpose of the information security audit is to assess the ITS security status and to develop recommendations for the application of a set of organizational measures and software tools aimed at securing the ITS information and other resources from threats to information security. During the audit of information security one of the tasks that is solved is the audit of ISMS. The current realities of information security systems design and construction require a focus on international standards and recommendations. Information security audit in the current environment is one of the most effective tools for obtaining an independent and objective assessment of the current level of security of any economic entity from both existing and potential threats. To achieve the aim of the master thesis goal, the following tasks are solved in the work:

1) determining the place of the ISMS audit in the information security system;

2) analysis of standards for auditing of ISMS and principles of auditing of ISMS;

3) research on the evaluation of the ISMS auditors and their competencies to meet the needs of the ISMS audit program;

4) exploring the basic principles of program development and the objectives of the ISMS audit;

5) analysis of leading guidance on managing the audit program;

6) the recommendations calculation of the

Thus, the paper elaborates a complex of questions on the ISMS audit, which in the aggregate and make up the Methodology for conducting an integrated audit of the ISMS to protect the information assets of the organization.

Finally, in the last few years, in connection with many hacking attacks, not only in enterprise information systems but also in the key state structures, the concept of "information security" has expanded to the concept of "cyber security". Cybersecurity is the process of using security measures to ensure the confidentiality, integrity, and accessibility of an organization's electronic data when attempting to knowingly damage not only the database but also the operating system of the server from multiple parties

(networks). Such measures apply not only to corporate information system, but also to the information communications networks and the environment in which the data is transmitted (hence the term cyber-environment). In other words, not only the local area networks of computers and servers are protected, but also buildings, personnel and the medium of communication (cables, communication lines with the corresponding equipment, receivers, transmitting stations, etc.).

The goal of cybersecurity is to ensure the most complete protection of your data (server) both in the process of transmission and / or exchange and in the process of their storage. Now in the Western countries cyber security training is planned already from the school bench. For example, in the UK, students will be offered lessons in which they will learn the skills that allow the security of British companies and organizations from online hacking attacks. The curriculum is developed by the UK Ministry of Culture, Media and Sport. The lessons are planned to be delivered both online and in the form of extracurricular classes, which will be held four times a week and will be conducted by teachersexperts. The program is aimed at students aged 14 to 18 years.

The Master's Thesis proposes the way of introducing an information security audit department in UIA. We have also calculated the costs of an internal audit and shown, that the procedure of internal audit is significantly less costly than ordering an external adit, if to be precise: internal ausdit is 1723 USD compared to approximate 38 thousand USD.

Internal audit can be conducted as often as the company has the need in it. Recommended frequence of internal audit is once a quarter. The results of the information security audit allow us to form strategic development settings that meet the current challenges of the information security system for the specified entity. However, it should be understood that the use of information security audits in practice should not be episodical, but regular, which allows not only to identify a fact already established, but also to anticipate potential threats.

REFERENCES

1. Georg Disterer. Journal of Information Security Vol.4 No.2, Article ID: 30059. ISO/IEC 27000, 27001 and 27002 for Information Security Management - 2013. - 9 p.

2. Robert R. Moeler. IT Audit, Control, And Security.- 2012. – 696 p.

3. E. Humphrey. Information Security Management System Standards, Datenschutz und Datensicherheit, Vol. 35, No. 1, 2011. – 40 p.

4. ISO 27002 - Information technology – Security techniques – Code of practice for information security controls.

5. Информационная безопасность (2-я книга социально-политического проекта «Актуальные проблемы безопасности социума. – 2009. – 124 ст.

6. Інформаційна безпека і кібербезпека - в чому різниця?. *indevlab.com* (uk). Процитовано 2019-10-17. [Online resource] – Access mode: https://indevlab.com/uk/blog-ua/informatsijna-bezpeka-i-kiberbezpeka-v-chomu-riznitsya/

7. Hans Baars, Jule Hintzbergen, Kees Hintzbergen, Andre Smulders. Foundations of Information Security Based on ISO27001 and ISO27002. – 2010. – 150 p.

8. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII

9. Understanding difference between Cyber Security & Information Security - CISO Platform by Amit, CISO Platform. [Online resource] – Access mode: https://www.cisoplatform.com/m/blogpost?id=6514552%3ABlogPost%3A47287

10. Sony Pictures Hack. [Online resource] – Access mode: https://en.wikipedia.org/wiki/Sony_Pictures_hack

11. Global Security Report Shows Majority of Companies Do Not Detect Breaches on Their Own. [Online resource] – Access mode: https://securityintelligence.com/news/global-security-report-shows-majority-of-companies-do-not-detect-breaches-on-their-own/

12. IBM technology. [Online resource] – Access mode: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEL03042USEN&attachment=SEL03042USEN.PDF

13. Obama targets foreign hackers and state-owned companies over cuber-attacks. [Online resource] – Access mode: http://www.theguardian.com/technology/2015/apr/01/obama-targets-foreign-hackers-state-owned-companies-sanctions

14. Fake iTunes Compromise MSS Treat Report. [Online resource] – Access mode: https://portal.sec.ibm.com/mss/html/en_US/support_resources/pdf/Fake_iTunes_Compromise_MSS_Threat_Report..pdf

15. Cyber Attacks Likely to Increase. [Online resource] – Access mode: http://www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/

16. Cyber attacks rise at critical infrastructure firms. [Online resource] – Access mode: http://www.cnet.com/news/cyber-attacks-rise-at-critical-infrastructure-firms/

17. Criminal Hackers Planning cyber Attacks. [Online resource] – Access mode: http://krebsonsecurity.com/wp-content/uploads/2013/05/DHSEM-01-SAU-02-UFOUO-HSN-OpUSA-Criminal-HackersPlanning-Cyber-Attacks-05012013.pdf

18. Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави, затверджений постановою Кабінету Міністрів України від 23 серпня 2016 р. № 563

19. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII

20. European Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

21. U.S. Government, White House, Homeland Security, Presidential Directive 7: *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003. [Online resource] – Access mode: http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#content .

22. Elgin Brunner and Manuel Suter, International CIIP Handbook 2008/2009: An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies. 2008. – 656p.

23. *[International CIIP Handbook 2008/2009*, Table 1; U.S. Department of Homeland Security, U.S. Department of the Interior: *National Monuments & Icons: Critical Infrastructure and Key Resources, Sector-Specific Plan*, 2010. [Online resource] – Access mode: www.dhs.gov/xlibrary/assets/nipp-ssp-national-monuments-icons.pdf

24. IATA (International Air Transport Association), Air Transport Facts, 2009. [Online resource] – Access mode: http://www.iata.org/pressroom/facts_figures/fact_sheets/Pages/economicsocial-benefits.aspx. The IATA represents 93 percent of scheduled air traffic in the world

25. Lior Tabansky, "Basic Concepts in Cyber Warfare," *Military and Strategic Affairs* 3, no. 1. – 2011. - 98p.

26. Whitehouse (2009) "Cyberspace Policy Review-Assuring a Trusted and Resilient Information and Communications Infrastructure"

27. European Commission(2013) "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

28. ENISA(2012a) *National Cyber Security Strategies: Setting the course for national efforts to strengthen in Cyberspace*

29. ENISA(2012b) *National Cyber Security Strategies: Practical Guide on Development and Execution*

30. ENISA(2013) REGULATION (EU) No 526/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 21 May 2013 concerning the European Union Agency for Network and Information Security

31. EP3R(2010) "NON-PAPER on the ESTABLISHMENT OF A EUROPEAN PUBLIC-PRIVATE PARTNERSHIP FOR RESILIENCE (EP3R)"

32. ECAC Policy Statement in the Field of Civil Aviation Security, 13th edition. - 2010. - 138 p.

33. Doc 8973, Aviation Security Manual, 10th edition, ICAO, 2017, 808 p.

34. R. Abeyratne, Aviation Security Law, DOI 10.1007/978-3-642-11703-9_6,

Springer-Verlag Berlin Heidelberg. - 2010. – 287 p.

35. ICAO Universal Security Audit Programme. [Online resource] – Access mode: https://caainternational.com/our-services/avsec/icao-universal-security-audit-programme/

36. ISO/IEC 27000 *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

37. ISO/IEC 27001 *«Information technology — Security techniques — Information security management systems — Requirements»*.

38. *Official website* of Ukraine International Airline. URL: https://www.flyuia.com/ua/en/home.

39. Конев, И. Р. Информационная безопасность предприятия / И. Р. Конев, А. В. Беляев. – СПб. : БХВ-Петербург, 2004. – 752 с. – ISBN 5-94157-280-8

40. LOUKIL, A. (2017, November 7-8). Joint ACAC/ICAO MID Workshop on GNSS . Last access date May 15, 2019, ICAO UNITING AVIATION: A UNITED NATIONS SPECIALIAZED AGENCY: [Online resource] – Access mode: https://www.icao.int/MID/Pages/2017/GNSS-Wksp.aspx

41. How to use Plan Do Check Act (PDCA) in Aviation Safaty Management. [Online resource] – Access mode: http://aviationsafetyblog.asms-pro.com/blog/how-to-use-plan-do-check-act-pdca-in-aviation-safety-management.

42. С. С. Ерохин и С. В. Голубев, «Основные этапы оценки защищенности объектов информационных систем. Электронные средства и системы управления», *5-я молодежной научно–практической конференции*, Томск, В–Спектр, сс. 51–53, 2009

43. Realising European Reselience for Critical Infrastracture. [Online resource] – Access mode: http://resilens.eu/about-resilience/critical-infrastructures/

44. Understanding the airport ecosystem. [Online resource] – Access mode: https://cyberstartupobservatory.com/aviation-cybersecurity-understanding-the-airport-ecosystem/