PRIVATE PROFESSIONAL EDUCATIONAL INSTITUTION

«KRASNOYARSK COOPERATIVE TECHNICAL SCHOOL OF ECONOMICS, COMMERCE AND LAW»

Inter-subject training project in the disciplines "MDK 01.05 Office management and secrecy regime" and "English language"

By topic: "Concepts and types of confidential information. Threats to the security of confidential information"

Учебный межпредметный проект по дисциплинам «МДК 01.05 Делопроизводство и режим секретности» и «Английский язык»

По теме: «Понятия и виды конфиденциальной информации. Угрозы безопасности конфиденциальной информации»

Completed by a student of the group: PDB-2(3)

Specialty: Law enforcement

Utyuzh Rostislav Yevgenyevich

Project manager: teacher of the highest qualification category Panasyuk Tatyana Vladimirovna.

Krasnoyarsk 2024

topic:

CONCEPTS AND TYPES OF CONFIDENTIAL INFORMATION. SECURITY THREATS TO CONFIDENTIAL INFORMATION

TABLE OF CONTENTS:

[Abstract 3](#_Toc164661842)

[Introduction 4](#_Toc164661843)

[1. Defining confidential information 6](#_Toc164661844)

[2. Main types of confidential information 7](#_Toc164661845)

[3. Conditions and types of security threats 9](#_Toc164661846)

[4. Confidential information protection tools 12](#_Toc164661847)

[Conclusion 13](#_Toc164661848)

[Source list 14](#_Toc164661849)

## Annotation

Topic: "Concepts and types of confidential information. Threats to the security of confidential information" is an overview of the concept of confidential information and its types. I will review the main types of information in the project and tell you in detail about confidential information, its types, subspecies, and features.

The project examines theoretical aspects of privacy, including the definition of confidential information, its meaning and role in the modern world. It also describes various types of confidential information, such as commercial, personal, government, and others.

It also discusses many important methods of protecting confidential information and its importance for various fields of activity, including business, law and public administration.

Keywords

Confidential information, secret, circle of persons, information leak, state secret, reasons, information protection, official secret, disclosure, conditions.

## Introduction

Relevance: The topic of confidential information is important and relevant in our information society, especially in the context of the increasing amount of digital data that is stored and processed. As more legal entities move to digital data storage for fast data transfer and work with data in the organization. Information exchange plays an important role in law enforcement activities for the interaction of structural divisions and employees within the organization. In a rapidly changing environment, it is also important to study new ways of information leakage and types of their storage.

Problem: The concepts and types of confidential information may be different and incomprehensible to employees due to the related definition. Information is divided into the types of access to it by certain persons and the number of persons who dispose of it. Ignorance of the type of confidential information and the rules for handling it leads to the main problem -a threat to the security of confidential information "data leaks" disclosure of confidential information to third parties.

Project goal: to ensure that employees of the organization understand the basic concepts and types of information, in particular confidential. Creating this goal will help reduce the risk of disclosing information to third parties, as well as improve understanding of the importance of certain information that is used within the organization; improve skills in working with professional vocabulary in English.

Project objectives:

- Systematization and analysis of scientific and practical literature;

- Defining the basic concepts of information and confidential information in accordance with the current federal law;

-Identification of security threats to confidential information;

-Analysis of the application of various types защиты of confidential data protection;

Hypothesis: effective protection of confidential information affects the work of law enforcement officers. Understanding the types of confidential information will help reduce the level of disclosure of such information to third parties. By studying various aspects of information legislation and identifying them, it is possible to identify methods for effective circulation of confidential information among employees.

 Method: collection and analysis of information, systematization and translation into English.

## 1. Definition of confidential information

From the beginning, it is necessary to disclose the concept of confidential information-this is information, regardless of the form of its provision, that cannot be transferred by a person who has obtained access to this information to third parties without the consent of their rightholder, or obtaining a special status.

When using данных data that has a special status, the problem of confidentiality inevitably arises, otherwise they will lose their value. Confidentiality of information is the preservation of integrity, protection against leakage of information that is not intended for general use and has intellectual and economic value for the owner. Organizational, legal, and technical measures are used to maintain confidentiality and protect information. In order for information to become confidential, its owner must be sure that it belongs to one of the described types listed in Presidential Decree No. 357 of 13.07.2015, or must independently label it "strictly confidential" and restrict access to it.

Types of confidential information:

It is considered that the typology of confidential information was established by Decree of the President of the Russian Federation No. 188 of March 6, 1997 "On the list of confidential information".

## 2. Main types of confidential information

The decree defines six types of confidential information, which are presented as follows:

1. Information about facts, events and circumstances of a citizen's private life that allow identifying his / her identity (personal data), with the exception of information subject to dissemination in the mass media in cases established by federal laws.

2. Information constituting the secret of the investigation and judicial proceedings.

3. Official information, access to which is restricted by state authorities in accordance with the Civil Code and federal laws (official secret).

4. Information related to professional activity, access to which is restricted in accordance with the Constitution and federal laws (medical, notarial, lawyer's secrets, secrets of correspondence, telephone conversations, mailings, telegraph or other messages, etc.).

5. Information related to commercial activities, access to which is restricted in accordance with the Civil Code and federal laws (commercial secret).

6. Information about the essence of the invention, utility model or industrial design before the official publication of information about them.

Personal data:

This type includes such personal information about people as date and place of birth, marital status, education, and work experience. They are considered confidential if the owner has not given permission for their public presentation in the media or on the Internet.

Official secret:

This type can be called complex, since it combines information that is restricted to access by state or federal authorities in accordance with current legislation. For example, this category includes investigative and judicial secrets, and military secrets. This also includes personal data about people who have opened up while performing their official duties.

Trade secret:

For the most part, these are data belonging to the company and its managers, which are used to conduct business and maintain its competitiveness. This includes information about the organization's credit history, annual turnover, employee salaries, in-house developments and new projects, and innovative technologies.

Professional secret:

This type contains information related to professional activity: medical, notarial, lawyer's secrets, inviolability of personal correspondence, telephone communication, and postal messages.

Information about the essence of the invention:

Most often, this is information that contains technical aspects, results of testing inventions, prototypes or samples before being presented to the public and put into mass production.

##

## 3. Conditions and types of security threats

In the course of the activity of an enterprise or organization, protected information may, for various reasons, fall out of the possession of the subjects who own it, or to whom it was entrusted, or became known through service or work. At the same time, the protected information goes beyond the limits of the established sphere of circulation, protected by special regime measures, and control over its distribution is lost – information leaks occur.

Before talking about security threats, you should determine the causes and conditions of their occurrence. The most common reasons for information leaks are:

- imperfection of regulatory acts regulating information protection;

- insufficient available forces and means to block the channels of information leakage;

- violation by persons authorized to work with protected information of the established rules for its protection.

These reasons lead to information leakage if appropriate subjective or objective conditions contribute to this.

Subjective conditions for information leakage include:

- the executors ' ignorance of regulatory acts on information security issues;

- poor educational and preventive work in the team;

- insufficient attention on the part of managers to the issues of ensuring the secrecy regime;

- weak control over the state of the secret storage system;

- decision-making by managers without taking into account the requirements of the secrecy regime.

Objective conditions for information leakage include:

- imperfection or absence of regulatory acts regulating the rules of information protection on certain issues;

- imperfection of the list of information subject to classification;

- turnover of personnel from high-security units;

- non-compliance of the premises with the requirements necessary for carrying out work with secret documents and products.

These reasons and conditions create prerequisites and opportunities for the formation of a leak channel for protected information. This concept should not be equated with a communication channel, which is a channel for transmitting information from one system to another.

And so now you can go to the threats themselves. In the course of the activity of an enterprise or organization, protected information may, for various reasons, fall out of the possession of the subjects who own it, or to whom it was entrusted, or became known through service or work. At the same time, the protected information goes beyond the limits of the established sphere of circulation, protected by special regime measures, and control over its distribution is lost – information leaks occur.

Such a term as "information leak" has long been fixed in the scientific literature and regulatory documents, but there is no single approach to defining this term.

At the same time, information leakage does not mean that it is received only by persons who do not work at the enterprise, unauthorized access to confidential information of employees of this enterprise can also lead to leakage.

Along with information leakage, such concepts as disclosure, disclosure and distribution of protected information, and unauthorized access to it should also be distinguished.

Types of threats:

-Disclosure of protected information is unauthorized access to such information by persons who do not have legal access to it, carried out by a person to whom this information was entrusted or became known through the service. Disclosure can be made among their colleagues who do not have access to this information, among relatives, acquaintances and other persons.

-Disclosure of protected information is its publication in the mass media, use in speeches at public conferences or symposiums by persons who have become aware of this information in the service.

-Distribution of protected information is the open use of information of limited distribution.

-Unauthorized access – obtaining access to protected information bypassing the security system by software, technical and other means, as well as due to accidental circumstances.

##

## 4. Confidential information protection tools

The security of confidential data information should be approached systematically, regardless of the method of its storage. For each type of information security, there are different methods of protecting it, which are divided into legal, organizational, and technical measures. However, these measures should work hand in hand in the overall package. The lack of necessary documents will not allow even the most reliable system to function. The organization's security service or individual specialists develop measures and ensure information protection.

Key measures to protect confidential information:

- Security of confidential information in a protected room intended for conducting confidential negotiations.

- Ensuring the protection of confidential information processed by technical means;

- Control of employees ' access to confidential information;

- Control over the movement of confidential information and its protection:

- Design of computerization objects in a secure version;

- Certification and annual control of informatization facilities according to security requirements.

## Conclusion

In conclusion, we can say that after analyzing the definition and types of confidential information. While working on the project, I identified the most important types of confidential information, defined them, and explained their content.

The study also found that security threats do not occur by themselves, so they are preceded by causes and conditions, which in turn are also divided into types. Based on this, we can say that you can protect information from all the types of threats that I mentioned in the project work at the stage of their "origin".

By this I want to say that all security measures should be focused on limiting the occurrence of conditions and causes of security threats, and not on preventing or detecting already committed "information leaks"

## List of sources

1)Federal Law No. 149-FZ of 27.07.2006 "On Information, Information Technologies and Information Protection "(latest version)

2)Federal Law No. 152-FZ of 27.07.2006 "On Personal Data "(latest version)

3) The Civil Code

4) The Code of Criminal Procedure

5)https://epp.genproc.gov.ru/web/proc\_78/activity/legal-education/explain/criminal\_proceedings?item=59137728

6)https://searchinform.ru/resheniya/biznes-zadachi/rabota-s-konfidentsialnoj-informatsiej/pravovoe-regulirovanie-konfidentsialnoj-informatsii/

7) Vikhorev S. V. "Confidential information and legislation of the Russian Federation " / Abstracts of a speech at the conference"Information Security". Vus M. A., Fedorov A.V. State Secret and its Protection in the Russian Federation, St. Petersburg: Law Center Press, 2020

8)<https://is.astral.ru/services/zashchita-informatsii/zashchita-konfidentsialnoy-informatsii/>