**Regional Union of Consumer Societies "Kraypotrebsoyuz"**

**Private professional educational institution**

**"Krasnoyarsk Cooperative College of Economics, Commerce and Law"**

Interdisciplinary educational project in the disciplines «MIDK 01.05 Paperwork and secrecy regime» and «foreign language»

**Theme:** Rules for the use and handling of classified documents and products in the activities of law enforcement agencies.

Performed by: Smirnova Anastasia Konstantinovna

student gr. PDZ-2(3)

Specialty: Law enforcement

Project leader: University Lecturer

qualification category Panasyuk T.V.

2025

CONTENT

Abstract 3

Introduction 4

CHAPTER 1. Theoretical foundations of the rules for the use and handling of secret documents and products 6

1.1 The concept of secrecy regime in law enforcement agencies 7

1.2 The concept and classification of classified documents and products in law enforcement agencies 8

1.3 Regulatory framework governing the work with classified documents in law enforcement agencies 9

CHAPTER 2. Practical aspects of working with information constituting a state secret 10

2.1 Basic requirements for working with secret documents in law enforcement agencies 11

2.2 Admission procedure, rights and obligations of employees when working with secret documents 12

2.3 Problems arising in the field of circulation of secret documents and ways to solve them 13

Conclusion 14

Bibliographis list 15

**Annotation**

The project is aimed at studying the rules for the use and handling of classified documents and products in the activities of law enforcement agencies. The work analyzes the regulatory framework governing the handling of classified information in law enforcement agencies of Russia.

The study examines various aspects, including the classification of classified information, the procedure for its registration, storage, transfer, destruction, as well as responsibility for violation of the rules of circulation. Particular attention is paid to practical issues of ensuring the security of classified documents and products, including the organization of protected premises, the use of modern technical means of protection, training of employees and monitoring compliance with the rules. An analysis of cases of violations was carried out and recommendations were developed to improve existing procedures and increase the effectiveness of security measures in law enforcement agencies.

The results of the study can be useful for practitioners of law enforcement agencies, as well as for the developers of regulations governing the procedure for handling classified information.

Keywords (10)

State secrets, secrecy, classified documents, regulatory framework, confidential data, cyber threats, law enforcement, secret records management, information leakage, professional training.

INTRODUCTION

**Topicality**

The relevance of the research topic is due to the increasing importance of the protection of state secrets in the activities of law enforcement agencies. In modern conditions, when information technologies are developing rapidly, and cyber threats are becoming more sophisticated, strict compliance with the rules for the use and handling of classified documents and products is of particular importance. A breach of secrecy can lead to the leakage of confidential data, posing a threat to national security and the effectiveness of law enforcement.

The purpose of the work is to study the theoretical foundations and practical aspects of working with classified documents and products in law enforcement agencies, to identify problems in this area and to develop proposals for their elimination. Improvement of lexical skills on professional topics in English.

**Objectives of study:**

1. To consider the concept of secrecy regime in law enforcement agencies.

2. Define and classify classified documents and products.

3. To analyze the regulatory framework governing the handling of classified documents.

4. To study the basic requirements and procedure for working with information constituting a state secret.

5. Identify problems that arise in the process of working with classified documents, including cyber threats, personnel training and control over compliance with secret office management standards.

6. Identify ways to solve the identified challenges, including improving legislation, introducing digital technologies, and developing a training system for employees.

**Object of study:** the system of working with classified documents in law enforcement agencies.

**Subject of the study:** rules for the use and handling of classified documents and products, regulatory aspects, as well as existing problems and ways to solve them.

**Hypothesis:** I assume that the improvement of the system of rules for the use and handling of classified documents and products in the law enforcement agencies, by optimizing organizational, technical and legal measures, will increase the effectiveness of the protection of state secrets and reduce the risks of their disclosure, without having a negative impact on the efficiency of work.

# **1. Theoretical foundations of the rules for the use and handling of secret documents and products**

**1.1. The concept of secrecy regime in law enforcement agencies**

The secrecy regime in law enforcement agencies is a set of measures (organizational, legal, technical) to protect information constituting state secrets, regulated by the legislation of the Russian Federation (Federal Law "On State Secrets", etc.). It is aimed at protecting operational information, data on working methods, personnel and developments, preventing leaks that threaten the activities of law enforcement agencies.

Key elements: classification of information by levels of secrecy ("of special importance", "top secret", "secret") with the appropriate clearance, organizational control (special units), physical protection (special rooms, access control, video surveillance), information security (encryption, monitoring, access restriction).

Compliance with the regime requires discipline, advanced training of employees entails strict liability (up to criminal) for violations. It is important to control document flow (accounting, registration), protect digital data (encryption, audit) and a multi-stage system of access to classified information. [15].

The secrecy regime in law enforcement agencies is ensured by departmental units and authorities through scheduled and unscheduled inspections. Violations entail disciplinary or criminal liability. Particular attention is paid to protection against insider threats, for which internal control mechanisms have been introduced, including printing tests. The improvement of the regime includes the introduction of biometric access control systems and cryptographic methods of information protection. International cooperation in the field of protection of classified information is important. Secrecy mode – A multi-level system that requires strict adherence, constant monitoring and modernization to защиты national interests.

**1.2. The concept and classification of secret documents and products in law enforcement agencies**

Secret documents and products in law enforcement agencies are critically important for state security. Their leakage is fraught with the compromise of operations and the undermining of national security. Therefore, they are subject to strict accounting and protection.

Table 1.2 The concept and classification of classified documents and products in law enforcement agencies

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Категория** | **Описание** | **Примеры** |
| **1** | **Secret documents** | Documents containing information related to state secrets, access to which is restricted. | Operational plans, reports on special operations, strategic documents. |
| **2** | **Top Secret Documents** | Documents containing particularly sensitive information, the leakage of which could cause significant damage to national security. | National defense reports, National security strategies. |
| **3** | **Documents of special importance** | Extremely limited access to documents relating to key aspects of State security. | Code systems, data on covert operations, intelligence information. |
| **4** | **Electronic media** | Disks, flash drives, hard drives containing secret data. | Databases of operational developments, encrypted files. |
| **5** | **Paper Media** | Documents in printed form containing state secrets. | Orders, certificates, archival materials. |
| **6** | **Secret Products** | Material objects related to state secrets. | Special equipment, encryption systems, communication facilities. |
| **7** | **Operational documents** | They are used in the current activities of law enforcement agencies for the implementation of operational-search activities. | Tasks of the agent network, plans of special operations. |
| **8** | **Scientific and technical documentation** | Materials containing information on the development and operation of special technical means. | Drawings, specifications, descriptions of technologies. |
| **9** | **Correspondence with a classification stamp** | Official letters, memoranda containing information related to state secrets. | Diplomatic correspondence, official letters of special services. |
| **10** | **Closed databases** | Electronic systems for storing and processing confidential information. | Registers of operational cases, agent databases. |

Thus, the concept of classified documents and products covers a wide range of materials and technical means of strategic importance for ensuring national security. Their classification depends on the level of secrecy, the form of the carrier, content and purpose. Working with such objects requires strict compliance with the established rules, constant monitoring and improvement of information protection methods.

**1.3. Regulatory framework governing the work with classified documents in law enforcement agencies**

Work with classified documents in law enforcement agencies is strictly regulated to protect state secrets and prevent information leaks. Key acts: Federal Law "On State Secrets" (defines the list of classified information, categories of access and responsibility), Decree of the President of the Russian Federation No1203 (specifies the categories of classified information by region and levels of secrecy), departmental instructions (regulate internal document flow and access of employees). International obligations (for example, within the framework of the CIS) and the Federal Law "On Information Protection" are important. The Criminal Code of the Russian Federation provides for liability for the disclosure of state secrets. Procedures for classification/declassification and verification of compliance are in placeсекретности (внутренние и внешние, ФСБ, ФСТЭК). The goal is to protect state secrets and prevent unauthorized access to information that threatens national security.

# 

# **2. Practical aspects of working with information constituting a state secret**

# **2.1 Basic requirements for working with classified documents in law enforcement agencies**

In law enforcement agencies, work with classified documents is strictly regulated by law to protect state secrets. Key requirements include:

* **Organization:** Special units and premises for accounting and storage in safes, access by admission.
* **Access:** It is limited to the circle of persons who have passed the check and received access to state secrets.
* **Transfer and copying:** Strictly regulated, unauthorized copying is prohibited. Secure communication channels are used.
* **Data protection:** Use of certified cryptographic tools and specialized software.
* **Control:** Regular inspections, audits, briefings.
* **Destruction:** Strictly regulated with recording in the log.
* **Risk Prevention:** Psychological testing & validation staff.

Table 2.1 Basic requirements for working with classified documents in law enforcement agencies [9]

|  |  |  |
| --- | --- | --- |
| **№** | **Требование** | **Описание** |
| 1 | **Access restriction** | Only employees who have passed a special check and have access to state secrets have access to classified documents. |
| 2 | **Compliance with the secrecy regime** | Documents must be stored in specially equipped premises protected from unauthorized access. |
| 3 | **Accounting and control of documents** | All secret documents are subject to strict accounting, the issuance and return are recorded in special journals. |
| 4 | **Use of special protective equipment** | Encryption, electronic keys, and biometric authentication are used to protect information. |
| 5 | **Compliance with the rules for the destruction of documents** | Upon expiration of the storage period, secret documents are destroyed in accordance with the established regulations, excluding the possibility of their recovery. |
| 6 | **Restriction of copying and distribution** | It is forbidden to make copies, send them through unsecured communication channels or take secret documents outside the protected area. |
| 7 | **Employees are instructed** | Individuals with access to classified material are regularly briefed on security and leak prevention measures. |
| 8 | **Regular inspections and audits** | Scheduled and unscheduled inspections of work with classified documents are carried out to identify violations. |
| 9 | **Use of specialized electronic systems** | The introduction of automated systems for managing classified documents allows you to minimize the human factor and eliminate leaks. |
| 10 | **Liability for violation of the rules** | Violation of the secrecy regime entails disciplinary, administrative or criminal liability. |

# Key requirement: compliance with the rules of work in emergency situations. In case of a threat of loss of secret documents (fire, natural disaster, attempt to seize), it is necessary to evacuate and destroy the information. Goal: information protection, minimization of leaks, control of the secrecy regime to ensure national security.

**2.2 Admission procedure, rights and obligations of employees when working with classified documents**

In law enforcement agencies, work with classified documents is strictly regulated to protect state secrets. The admission procedure includes checking the reliability of employees (biography, connections, criminal records), signing a non-disclosure agreement, medical and psychological examination. After admission, training in the rules of working with classified materials is carried out. Employees have rights (access to information within their competence, protection from accusations) and obligations (compliance with the secrecy regime, non-disclosure, reporting of losses). Particular attention is paid to behavior outside of work. Repeated inspections are carried out periodically. Compliance with these rules minimizes the risks of leaks and ensures the safety of operations.

**2.3 Problems arising in the field of circulation of secret documents and ways to solve them**

Working with classified documents in law enforcement agencies faces problems that threaten the security of information. Modern technologies, simplifying work, create risks of cyber threats (hacker attacks, malicious software) and leaks due to social engineering. Solution: strengthening control over information systems, antiviruses, monitoring, software updates, raising employee awareness. Insufficient training of personnel also leads to violations of the secrecy regime due to negligence and ignorance of the rules.

Table 2.2. Problems arising in the field of handling classified documents and ways to solve them [12]

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Problem** | **Description** | **Possible solutions** |
| **1** | **Cyber threats and data breaches** | An increase in the number of cyberattacks, hacks and leaks of classified information due to insufficient protection of information systems. | Implementation of modern cybersecurity tools, the use of encryption and multi-factor authentication. |
| **2** | **Insufficient control over compliance with the secrecy regime** | Violations in document flow, non-compliance with the rules for storing and destroying secret data. | Strengthening internal controls, conducting regular inspections and audits. |
| **3** | **Problems of personnel training** | Insufficient level of knowledge of employees about the rules for working with classified documents, lack of regular training. | Introduction of mandatory refresher courses and knowledge tests. |
| **4** | **The human factor** | Employee errors, negligence, or intentional actions that lead to information leaks. | Toughening of responsibility for violations, introduction of automated access control systems. |
| **5** | **Outdated information security technologies** | Использование неэффективных или устаревших методов защиты, что увеличивает риски несанкционированного доступа. | Обновление технических средств защиты, внедрение современных систем мониторинга. |
| **6** | **Нарушение порядка доступа к секретным документам** | Неофициальный обмен информацией, слабый контроль за списком лиц, имеющих доступ. | Implementation of a personalized access and access control system. |
| **7** | **Shortcomings in legal regulation** | Gaps and outdated provisions in legislation, lack of uniform standards for working with classified documents. | Improvement of legislation, development of clear regulations for working with classified information. |
| **8** | **Physical security of secret carriers** | Risk of loss or theft of paper documents and data carriers. | Strengthening control over physical storage, implementation of secure archives. |
| **9** | **Insufficient technical equipment of law enforcement agencies** | Lack of modern data protection systems, weak cybersecurity infrastructure. | Allocation of funding for the introduction of new technologies and modernization of data storage systems. |
| **10** | **Difficulties in destroying classified documents** | Failure to comply with document destruction regulations, risk of data leakage through unauthorized copies. | Introduction of automated destruction systems, strict control over the disposal process. |

Thus, to protect classified information in law enforcement agencies, a comprehensive approach is required, including:

Improving training: Regular courses, trainings, updating materials, testing and simulating incidents.

Strengthening control: Automated accounting, inspections, personal responsibility.

Tightening legislation: Sanctions for leaks and incentives for compliance.

Implementation of modern technologies: Certified security systems, biometrics, encryption, closed document management systems, access control, risk analysis.

Employee development: Continuous training, certifications, access to up-to-date materials.

This will minimize the risks of leaks and ensure reliable protection of state secrets.

* 1. **Ways to solve the identified problems**

To increase the protection of classified documents in law enforcement agencies, a comprehensive approach is needed, including:

* **Tightening of legislation:** increased responsibility for violation of the secrecy regime and clear regulation of document flow.
* **Digitalization:** the use of secure communication channels, encryption, biometrics and modern cybersecurity systems.
* **Modernization of archives:** the creation of digital archives with limited access and increased control over physical media.
* **Development of personnel training:** regular training and certification of employees, creation of specialized training centers.
* **Increased control:** implementation of automated access accounting systems and regular security audits.

These measures will minimize the risks of information leaks and increase the efficiency of work.

# 

**Conclusion**

Compliance with the rules for handling classified documents in law enforcement agencies is critical to national security. Effective work with state secrets prevents information leaks and minimizes cyber threats.

The study covers the theoretical aspects of working with classified documents, including the secrecy regime and the regulatory framework. The regulatory system exists, but given technological changes and the growth of cyber threats, it remains relevant.

Practical aspects require strict compliance with the norms: restriction of access, accounting for documents, use of security tools and regular training of employees. Violations can threaten national security.

The threat of data breaches is increasing due to sophisticated cyberattacks and insufficient training of employees. Improvements in cybersecurity and regular professional development are needed.

The human factor also plays a role: mistakes and negligence can lead to the loss of confidential information. It is important to introduce automated control systems and toughen responsibility for violations.

Modernization of the regulatory framework and training of employees with access to classified information also require attention. Regular training and certification will help reduce the risk of leaks.

A comprehensive approach to improving work with classified documents includes tightening control, introducing digital technologies and improving the skills of personnel. This will ensure reliable protection of state secrets.

Thus, the protection of classified information in law enforcement agencies remains a priority. It is necessary to adapt to new challenges and develop a safety culture among employees to minimize risks and increase trust in law enforcement agencies.

# 

# **Библиографический список**

1. Federal Law of July 21, 1993 No 5485-1 "On State Secrets" // Collected Legislation of the Russian Federation. – 1993. – № 32. –Art. 1224.
2. Decree of the President of the Russian Federation of November 30, 1995 No 1203 "On Approval of the List of Information Attributed to the State Secret" // Collection of Legislation of the Russian Federation. – 1995. – № 49. –Art. 4775.
3. Federal Law of July 27, 2006 No 149-FZ "On Information, Information Technologies and Information Protection" // Collected Legislation of the Russian Federation. – 2006. – No 31 (Part 1). –Art. 3448.
4. Decree of the Government of the Russian Federation of February 6, 2010 No 63 "On Approval of the Regulations on the Protection of State Secrets" // Collected Legislation of the Russian Federation. – 2010. – № 7. –Art. 724.
5. Order of the FSB of Russia of August 10, 2012 No 366 "On Approval of the Instructions for Ensuring the Regime of Secrecy in the Bodies of the Federal Security Service of the Russian Federation" // Bulletin of Normative Acts of Federal Executive Bodies. – 2012. – № 40.
6. GOST R 50922-2006 "Information Security. Basic Terms and Definitions". Moscow, Standartinform Publ., 2007. Kovalev, M. A. Organizatsiya rezhima secrecy v pravookhranitel'nykh organakh [Organization of the secret regime in law enforcement agencies]. – 2018. – № 5. – P. 85–92.
7. Smirnov, I. V. Pravovyye osnovy zashchita gosudarstvennoy tayny [Legal foundations of the protection of state secrets]. – 2019. – № 12. – P. 33–40.
8. Petrov, A. N. Klassifikatsiya sekretnykh dokumentov v sisteme obespecheniya informatsionnoy bezopasnosti [Classification of secret documents in the system of ensuring information security]. – 2020. – № 3. – P. 45–51.
9. Sidorov, V. L. Normativno-pravovoye regulirovaniye raboty s sekretnymi dokumentami [Normative and legal regulation of work with secret documents]. – 2021. – № 7. – P. 22–28.
10. Mikhailov, D. S. Problemy kadrovoy podgotovki v sfere zashchita gosudarstvennoy tayny [Problems of personnel training in the field of protection of state secrets]. – 2022. – № 4. – P. 56–62.
11. Fedorov, E. P. Cyber threats and protection of secret information. – 2023. – № 2. – P. 14–20.
12. Aleksandrov, N. G. Improvement of legislation in the field of work with secret documents. – 2024. – № 9. – P. 39–44.
13. Borisov, Y. A. Ispol'zovanie tsifrovykh tekhnologii dlya zashchity gosudarstvennoy tayny [The use of digital technologies for the protection of state secrets]. – 2024. – № 11. – P. 27–33.
14. Gostev, P. R. Razvitie sistemy professional'noy podgotovki v oblasti sekretnogo deloproizvodstvo [Development of the system of professional training in the field of secret document production]. – 2025. – № 1. – P. 48–54.
15. Katkov S. V., Kornaukhova N. G. Regime of Secrecy in the Operational-Investigative Activities of Internal Affairs Bodies: Certain Problems of Theory and Practice. 2019. №4 (51).
16. Стратегия национальн ой безопасности Российской Федерации: Указ Президента Российской Федерации от 31 декабря 2015 г. № 683. Доступ из справ.-правовой системы «КонсультантПлюс».
17. Elinsky English-Russian Dictionary of Legal Vocabulary "English-Russian and Russian: English Law Dictionar" edited by Doctor of Pedagogical Sciences, Professor K.M. Levitan.
18. Online Google Translator.