**Частное профессиональное образовательное учреждение “Красноярский кооперативный техникум экономики, коммерции и права”**

Учебный межпредметный профессиональный проект по дисциплинам “МДК 01.05. Делопроизводство и режим секретности” и “Английский язык”.

По теме: Субъекты защиты информации в правоохранительных органах.

Выполнила студентка группы: ПДА-2(3)

Специальность: “Правоохранительная деятельность”

Ткаченко Арина Юрьевна

Руководитель проекта:

Преподаватель высшей квалификационной категории

Панасюк Татьяна Владимировна

Красноярск 2025

**СОДЕРЖАНИЕ**

Аннотация..........................................................................................................3

1. Введение.........................................................................................................4

1.1. Актуальность темы.....................................................................................5

1.2. Цели и задачи исследования......................................................................6

1.3. Методология исследования.......................................................................7

2. Понятие и классификация субъектов защиты информации......................8

2.1. Классификация субъектов в правоохранительных органах...................9

3. Правовые основы защиты информации в правоохранительных органах..............................................................................................................9

3.1. Международные стандарты и соглашения.............................................9

3.2. Роль правоохранительных органов в обеспечении информационной безопасности....................................................................................................10

Заключение......................................................................................................11

Список использованных источников............................................................12

**АННОТАЦИЯ**

В данной проектной работе исследуются субъекты защиты информации в правоохранительных органах, их роли и функции в процессе обеспечения безопасности данных. Актуальность выбранной темы обусловлена возрастающими угрозами утечек информации и необходимостью эффективного функционирования систем защиты информации в условиях современного информационного общества.

Основное внимание уделяется классификации субъектов защиты информации, включая государственные организации, правоохранительные органы, коммерческие структуры и частных граждан. Рассматриваются их полномочия, ответственность и взаимодействие в сфере защиты информации. Также анализируются механизмы, которые позволяют данным субъектам эффективно выполнять свои функции, такие как законодательные инициативы, технологические решения и организационные меры.

В процессе исследования использованы как теоретические, так и практические подходы, включая анализ существующих нормативно-правовых актов, изучение статистики утечек информации и обзор лучших практик в области информационной безопасности. В работе также предложены рекомендации по совершенствованию механизмов защиты информации, направленные на оптимизацию взаимодействия субъектов.

**КЛЮЧЕВЫЕ СЛОВА**

Защита информации, правоохранительные органы, субъекты защиты, информационная безопасность, киберугрозы, нормативно-правовые акты, конфиденциальность, государственная тайна, утечка информации, взаимодействие субъектов, технологические решения.

**ВВЕДЕНИЕ**

Современное общество характеризуется стремительным развитием информационных технологий, что неизбежно приводит к изменению подходов к защите информации. В условиях глобальной цифровизации и значительного увеличения объема данных, требующих защиты, правоохранительные органы играют ключевую роль в обеспечении информационной безопасности государства. ***Актуальность*** темы данной проектной работы определяется необходимостью глубокого анализа функций и полномочий субъектов защиты информации в правоохранительных структурах, в условиях постоянного увеличения киберугроз и современных вызовов. На фоне глобализации и интеграции информационных систем, проникновение в них злонамеренных элементов становится все более сложной и многогранной проблемой.

***Целью*** данной работы является исследование роли различных субъектов защиты информации в правоохранительных органах, а также анализ существующих механизмов и инструментов, направленных на обеспечение безопасности данных. В работе будут рассмотрены следующие ***аспекты***: классификация субъектов защиты информации; их полномочия и ответственность; взаимодействие между различными структурами в сфере информационной безопасности; оценка угроз и рисков, с которыми сталкиваются правоохранительные органы.

***Задачи исследования включают:***

1. Изучение законодательства, регламентирующего защиту информации в правоохранительных органах.

2. Анализ существующих программ и технологий защиты данных.

3. Выявление проблем и недостатков в деятельности субъектов защиты информации.

4. Разработка рекомендаций по улучшению механизмов защиты информации в правоохранительных органах.

Таким образом, ***результаты*** данной работы смогут внести вклад в существующее знание о защите информации, а также послужат основой для дальнейших исследований в данной области. В условиях стремительных изменений в сфере технологий и безопасности, вопрос о надежной защите информации остается особенно актуальным, и его исследование является необходимым для повышения эффективности работы правоохранительных органов.

**АКТУАЛЬНОСТЬ ТЕМЫ**

1. *Возрастание количества и сложности киберугроз:*

* Правоохранительные органы (ПO) становятся все более привлекательной целью для киберпреступников. Это связано с тем, что ПO хранят и обрабатывают огромные объемы конфиденциальной информации о гражданах, оперативной деятельности, расследованиях и т.д.
* Успешные кибератаки могут привести к утечке чувствительных данных, компрометации расследований, подрыву доверия общественности и даже угрозе национальной безопасности.
* Современные киберугрозы становятся все более изощренными, используя сложные техники.

*2. Цифровизация правоохранительной деятельности:*

* Современные ПO все больше полагаются на цифровые технологии для сбора, обработки, хранения и обмена информацией. Это включает в себя использование баз данных, систем видеонаблюдения, мобильных устройств, социальных сетей и облачных сервисов.
* Увеличение зависимости от цифровых технологий создает новые поверхности атаки и повышает риски информационной безопасности.

*3. Законодательные и нормативные требования:*

* Законодательство в области защиты информации (например, законы о персональных данных, о государственной тайне, о коммерческой тайне) накладывает строгие требования на ПO в отношении обработки и защиты информации.
* Несоблюдение этих требований может привести к юридическим последствиям, включая штрафы, иски и уголовную ответственность.
* ПO обязаны разрабатывать и внедрять эффективные меры защиты информации для соответствия законодательству.

**ЦЕЛИ И ЗАДАЧИ ИССЛЕДОВАНИЯ**

*Цель исследования* — выявить основные субъекты и меры защиты информации в правоохранительных органах, а также оценить их эффективность.

Некоторые *задачи*, которые могут входить в состав исследования:

* Анализ законодательных актов, касающихся защиты информации в правоохранительных органах. Необходимо рассмотреть роль законодательства в формировании мер безопасности и их влияние на эффективность работы систем информационной безопасности.
* Оценка современных угроз информационной безопасности в сфере правоохранительных органов. Следует проанализировать внешние киберугрозы и внутренние инсайдерские риски, обсудить примеры инцидентов и их последствия для системы работы органов.
* Исследование практики применения ГОСТа «Защита информации». Нужно описать влияние стандарта на процессы защиты данных и соответствие современным требованиям безопасности.
* Разработка рекомендаций по усовершенствованию защиты информации. Рекомендации формулируются на основе анализа современных угроз и существующих мер безопасности.
* Изучение перспективных технологий и инновационных решений для повышения уровня информационной безопасности в правоохранительных органах. Следует рассмотреть технические средства и организационные методы внедрения технологий.

**МЕТОДОЛОГИЯ ИССЛЕДОВАНИЯ**

В качестве *методологии исследования* могут использоваться, например, следующие подходы:

* Формально-логическое описание. Этот метод позволяет разработать описание ситуации как объекта познания, использовать его в процессе исследования, достичь иллюстративных целей и частично формализовать описание ситуации в терминах информационных технологий.
* Иерархический подход. Он предполагает описание механизма противоправных действий в отношении информации правоохранительных органов на трёх уровнях: концептуальном, процедурном и функциональном.
* Математическое моделирование. Такие методы используют для оценки эффективности механизмов защиты информации, например, от воздействия вредоносных программ.
* Использование научной литературы. В исследовании могут применяться работы в области системного анализа, информационной безопасности, криминалистики, уголовно-правовых и других наук.
* Анкетирование. В качестве эмпирической базы исследования могут использоваться результаты анкетирования сотрудников различных служб по вопросам организации защиты конфиденциальных сведений в органах внутренних дел.

**ПОНЯТИЕ И КЛАССИФИКАЦИЯ СУБЪЕКТОВ ЗАЩИТЫ ИНФОРМАЦИИ**

Субъекты защиты информации в правоохранительных органах — это различные участники деятельности по обеспечению информационной безопасности сотрудников органов внутренних дел (ОВД).

*Некоторые из них:*

* *Государство.* Основной субъект обеспечения информационной безопасности, который осуществляет свои функции через органы законодательной, исполнительной и судебной власти.
* *Негосударственные субъекты*. К ним относятся общественные формирования, содействующие органам правопорядка, например, общественные объединения, ветеранские организации.
* *Граждане, не являющиеся сотрудниками ОВД.* Их роль в обеспечении информационной безопасности заключается в создании благоприятных условий для выполнения сотрудниками ОВД возложенных на них задач.
* *Руководители органов, учреждений и организаций системы МВД.* Они несут персональную ответственность за организацию и состояние работы по обеспечению информационной безопасности сотрудников ОВД в подчинённых подразделениях.
* *Подразделения и должностные лица ОВД,* которые обеспечивают информационную безопасность сотрудников ОВД.

**КЛАССИФИКАЦИЯ СУБЪЕКТОВ В ПРАВООХРАНИТЕЛЬНЫХ ОРГАНАХ**

Классификация субъектов правоохранительных органов. Некоторые группы субъектов:

* *Государственные субъекты.* К ним относятся органы законодательной, исполнительной и судебной власти, структурные подразделения и должностные лица, наделённые определёнными полномочиями в сфере обеспечения информационной безопасности.
* *Негосударственные субъекты.* К ним относятся общественные формирования, содействующие органам правопорядка, например, общественные объединения, ветеранские организации.
* *Граждане, не являющиеся сотрудниками правоохранительных органов.* Их роль в обеспечении информационной безопасности заключается в создании благоприятных условий для выполнения сотрудниками их задач.

**МЕЖДУНАРОДНЫЕ СТАНДАРТЫ И СОГЛАШЕНИЯ**

Международные стандарты и соглашения, связанные с защитой информации в правоохранительных органах:

* Конвенция Совета Европы «О защите лиц в связи с автоматизированной обработкой персональных данных» 1981 года.
* Эталонная модель взаимодействия открытых систем (ЭМВОС), принятая по линии Международной организации стандартизации (ISO) в 1983 году. Описывает и регламентирует структуру и стандарты взаимодействия открытых систем для организации надёжного информационного обмена.
* «Руководящие принципы» ОЭСР. Являются минимальными стандартами, созданными в результате поиска консенсуса между позициями стран-членов ОЭСР по этому вопросу.
* Африканская конвенция о кибербезопасности и защите персональных данных от 27 июня 2014 года.
* Протокол о взаимодействии государств — членов Организации Договора о коллективной безопасности по противодействию преступной деятельности в информационной сфере от 23 декабря 2014 года.
* Инструментарий для законодательства о киберпреступности, разработанный Международным союзом электросвязи.
* Резолюции Генеральной Ассамблеи ООН, направленные на борьбу с преступным использованием информационных технологий (например, резолюции 55/63 от 4 декабря 2000 года и 56/121 от 19 декабря 2001 года).

**РОЛЬ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Правоохранительные органы играют *важную роль* в обеспечении информационной безопасности личности, общества и государства.

Некоторые *аспекты* роли правоохранительных органов в обеспечении информационной безопасности:

* *Защита информации*. Основная задача — предотвратить несанкционированный доступ, уничтожение, копирование или изменение данных. Также важно защищать информацию от утечки, так как это может нанести ущерб как самим правоохранительным органам, так и гражданам.
* *Противодействие киберпреступлениям*. Преступления с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации представляют серьёзную угрозу национальной безопасности. Правоохранительные органы борются с киберпреступностью, в том числе проводят анализ данных в информационно-телекоммуникационных сетях для выявления запрещённого контента.
* *Контроль доступа к информации.* Правоохранительные органы применяют системы контроля доступа к информационным системам, которые позволяют разграничить уровни прав доступа для сотрудников в зависимости от их должностных обязанностей и уровня допуска к секретной информации.
* *Физическая защита серверов и оборудования.* Это важно для защиты от несанкционированного проникновения к физическим носителям информации.

**ЗАКЛЮЧЕНИЕ**

Защита информации в правоохранительных органах важна для обеспечения национальной безопасности и эффективности правоприменительной деятельности. Для сохранности информации используются различные технические, организационные и правовые меры. Нормативно-правовая база защиты опирается на Конституцию РФ, Федеральные законы, Уголовный и Гражданский кодекс.

Существуют внешние и внутренние угрозы для информационной безопасности правоохранительных органов. К внешним угрозам относят деятельность служб разведки других государств, преступных сообществ, организаций, которые собирают сведения о деятельности правоохранительных органов. К внутренним угрозам — нарушение регламента сбора, обработки, хранения и передачи сведений, сбои в информационных системах и ошибки персонала.

Обучение сотрудников играет значительную роль в обеспечении информационной безопасности. Часто нарушения происходят из-за ошибок и недостатков в работе персонала.

Защита конфиденциальной информации в органах внутренних дел сформирована не до конца. Есть нюансы, которые мешают дальнейшему развитию системы защиты данных от несанкционированного использования и распространения.

Совершенствование системы защиты позволит повысить эффективность деятельности правоохранительных органов и обеспечить более сильную защиту общества и государства от преступных и других противоправных действий.

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

* Белоглазов Е. Г. и др. Основы информационной безопасности органов внутренних дел: учебное пособие. — М.: МосУ МВД России, 2012.
* Информационная безопасность в деятельности органов внутренних дел Российской Федерации: учебное пособие / под ред. Попова М. В. — М.: ЮСИЦ «ИГДИ», 2017.
* Лебедев В. Н. и др. под ред. Кирина В. И. Защита информации: учебник в 2-х частях. — Академия управления МВД России, 2013.
* Н. И. Журавленко, В. Е. Кадулин, К. К. Борзунов. Основы информационной безопасности: учебное пособие. — М.: МосУ МВД России, 2012.
* Руководство по информационной безопасности для правоохранительных органов: учебное пособие / под ред. Смирнова А. А. — М.: ЮНИТИ-ДАНА, 2020.
* Федеральный закон Российской Федерации №149 от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации».
* Постановление №1233 Правительства Российской Федерации от 03.11.94 «О порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».
* Федеральный закон Российской Федерации №125 от 27.07.2006 г. «О персональных данных».
* Приказ МВД РФ от 24.12.2008 г. №1138 «Об утверждении Кодекса профессиональной этики сотрудника органов внутренних дел Российской Федерации».

**Private Vocational Educational Institution "Krasnoyarsk Cooperative Technical School of Economics, Commerce and Law"**

Educational interdisciplinary professional project in the disciplines "MDK 01.05. Records Management and Secrecy Regime" and "English Language".

On the subject: Subjects of information protection in law enforcement agencies.

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

Specialty: "Law Enforcement"

Tkachenko Arina Yurievna

Project Manager:

Teacher of the highest qualification category

Panasyuk Tatyana Vladimirovna

Krasnoyarsk 2025

**CONTENT**

Annotation.......................................................................................................... 3

1.Introduction......................................................................................................4

1.1. Relevance of the topic.....................................................................................................................5

1.2. Goals and objectives of the study................................................................................................................... 6

1.3. Research methodology................................................................................ 6

2. The concept and classification of subjects of information protection............................................................................................................ 7

2.1. Classification of subjects in law enforcement agencies.............................. 8

3. Legal basis for information protection in law enforcement agencies............................................................................................................. 8

3.1. International standards and agreements..................................................... 8

3.2. The role of law enforcement agencies in ensuring information security............................................................................................................. 9

Conclusion........................................................................................................ 10

List of references.............................................................................................. 11

**ANNOTATION**

In this project work, the subjects of information protection in law enforcement agencies, their roles and functions in the process of ensuring data security are investigated. The relevance of the chosen topic is due to the growing threats of information leaks and the need for the effective functioning of information security systems in the modern information society.

The main attention is paid to the classification of subjects of information protection, including government organizations, law enforcement agencies, commercial structures and private citizens. Their powers, responsibilities and interaction in the field of information protection are considered. It also analyzes the mechanisms that allow these entities to effectively perform their functions, such as legislative initiatives, technological solutions and organizational measures.

In the course of the study, both theoretical and practical approaches were used, including the analysis of existing regulatory legal acts, the study of information leakage statistics and a review of best practices in the field of information security. The paper also offers recommendations for improving information security mechanisms aimed at optimizing the interaction of subjects.

**KEYWORDS**

Information protection, law enforcement agencies, subjects of protection, information security, cyber threats, regulatory legal acts, confidentiality, state secrets, information leakage, interaction of subjects, technological solutions.

**INTRODUCTION**

Modern society is characterized by the rapid development of information technologies, which inevitably leads to a change in approaches to information protection. In the context of global digitalization and a significant increase in the amount of data that needs to be protected, law enforcement agencies play a key role in ensuring the information security of the state. The relevance of the topic of this project work is determined by the need for an in-depth analysis of the functions and powers of the subjects of information protection in law enforcement agencies, in the context of a constant increase in cyber threats and modern challenges. Against the background of globalization and the integration of information systems, the penetration of malicious elements into them is becoming an increasingly complex and multifaceted problem.

The purpose of this work is to study the role of various subjects of information protection in law enforcement agencies, as well as to analyze existing mechanisms and tools aimed at ensuring data security. The following aspects will be considered in the work: classification of subjects of information protection; their powers and responsibilities; interaction between various structures in the field of information security; assessment of threats and risks faced by law enforcement agencies.

The objectives of the study include:

1. Study of legislation regulating the protection of information in law enforcement agencies.

2. Analysis of existing data protection programs and technologies.

3. Identification of problems and shortcomings in the activities of information security subjects.

4. Development of recommendations for improving information protection mechanisms in law enforcement agencies.

Thus, the results of this work can contribute to the existing knowledge about information security, as well as serve as a basis for further research in this area. In the context of rapid changes in the field of technology and security, the issue of reliable information protection remains especially relevant, and its study is necessary to improve the effectiveness of law enforcement agencies.

**RELEVANCE OF THE TOPIC**

Increasing number and sophistication of cyber threats:

* Law enforcement agencies (POs) are becoming an increasingly attractive target for cybercriminals. This is due to the fact that POs store and process huge amounts of confidential information about citizens, operational activities, investigations, etc.
* Successful cyberattacks can lead to the leakage of sensitive data, compromise investigations, undermine public trust, and even threaten national security.
* Today's cyber threats are becoming more sophisticated, using sophisticated techniques.

2. Digitalization of law enforcement:

* Today's POs are increasingly relying on digital technologies to collect, process, store, and share information. This includes the use of databases, video surveillance systems, mobile devices, social media, and cloud services.
* Increasing reliance on digital technologies creates new attack surfaces and increases information security risks.

3. Legal and regulatory requirements:

* Legislation in the field of data protection (e.g. laws on personal data, on state secrets, on trade secrets) imposes strict requirements on the Software with regard to the processing and protection of information.
* Failure to comply with these requirements can result in legal consequences, including fines, lawsuits, and criminal liability.
* POs are required to develop and implement effective information security measures to comply with the law.

**GOALS AND OBJECTIVES OF THE STUDY**

The purpose of the study is to identify the main subjects and measures of information protection in law enforcement agencies, as well as to assess their effectiveness.

Some tasks that may be included in the study:

* Analysis of legislative acts related to the protection of information in law enforcement agencies. It is necessary to consider the role of legislation in the formation of security measures and their impact on the effectiveness of information security systems.
* Assessment of modern threats to information security in the field of law enforcement agencies. It is necessary to analyze external cyber threats and internal insider risks, discuss examples of incidents and their consequences for the system of work of bodies.
* Study of the practice of applying GOST "Information Security". You need to describe the impact of the standard on data protection processes and compliance with modern security requirements.
* Development of recommendations for improving information security. Recommendations are formulated based on an analysis of current threats and existing security measures.
* Study of promising technologies and innovative solutions to improve the level of information security in law enforcement agencies. The technical means and organizational methods of technology implementation should be considered.

**RESEARCH METHODOLOGY**

For example, the following approaches can be used as research methodology:

* Formal-logical description. This method makes it possible to develop a description of the situation as an object of cognition, to use it in the process of research, to achieve illustrative goals and to partially formalize the description of the situation in terms of information technology.
* Hierarchical approach. It involves a description of the mechanism of illegal actions in relation to information of law enforcement agencies at three levels: conceptual, procedural and functional.
* Mathematical modeling. Such methods are used to assess the effectiveness of information protection mechanisms, for example, against the effects of malware.
* Use of scientific literature. The research can apply works in the field of system analysis, information security, forensics, criminal law and other sciences.
* Survey. As an empirical base of the study, the results of a survey of employees of various services on the organization of protection of confidential information in the internal affairs bodies can be used.

**CONCEPT AND CLASSIFICATION OF SUBJECTS OF INFORMATION PROTECTION**

Subjects of information protection in law enforcement agencies are various participants in the activities to ensure the information security of employees of internal affairs bodies (OVD).

Some of them are:

* State. The main subject of information security, which performs its functions through the legislative, executive and judicial authorities.
* Non-State actors. These include public formations that assist law enforcement agencies, for example, public associations, veteran organizations.
* Citizens who are not employees of the Department of Internal Affairs. Their role in ensuring information security is to create favorable conditions for the performance of the tasks assigned to them by police officers.
* Heads of bodies, institutions and organizations of the Ministry of Internal Affairs. They are personally responsible for the organization and state of work to ensure the information security of internal affairs officers in subordinate units.
* Units and officials of the Department of Internal Affairs who ensure the information security of employees of the Department of Internal Affairs.

**CLASSIFICATION OF SUBJECTS IN LAW ENFORCEMENT AGENCIES**

Classification of subjects of law enforcement agencies. Some groups of subjects:

* State actors. These include legislative, executive and judicial authorities, structural divisions and officials endowed with certain powers in the field of information security.
* Non-State actors. These include public formations that assist law enforcement agencies, for example, public associations, veteran organizations.
* Citizens who are not law enforcement officers. Their role in ensuring information security is to create favorable conditions for employees to perform their tasks.

**INTERNATIONAL STANDARDS AND AGREEMENTS**

International standards and agreements related to the protection of information in law enforcement agencies:

* Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981.
* The Open Systems Interoperability Reference Model (EMOS), adopted by the International Organization for Standardization (ISO) in 1983. Describes and regulates the structure and standards of open systems interoperability for the organization of reliable information exchange.
* OECD Guidelines. They are minimum standards created as a result of a search for consensus among the positions of OECD member countries on this issue.
* African Convention on Cybersecurity and Protection of Personal Data of June 27, 2014.
* Protocol on Cooperation of the Member States of the Collective Security Treaty Organization in Countering Criminal Activities in the Information Sphere of December 23, 2014.
* Toolkit for cybercrime legislation developed by the International Telecommunication Union.
* UN General Assembly resolutions aimed at combating the criminal misuse of information technologies (e.g., resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001).

**THE ROLE OF LAW ENFORCEMENT AGENCIES IN ENSURING INFORMATION SECURITY**

Law enforcement agencies play an important role in ensuring the information security of the individual, society and the state.

Some aspects of the role of law enforcement agencies in ensuring information security:

* Data protection. The main task is to prevent unauthorized access, destruction, copying or modification of data. It is also important to protect information from leakage, as this can be detrimental to both law enforcement agencies and citizens.
* Countering cybercrime. Crimes involving the use of information and telecommunication technologies or in the field of computer information pose a serious threat to national security. Law enforcement agencies are fighting cybercrime, including analyzing data in information and telecommunication networks to identify prohibited content.
* Control of access to information. Law enforcement agencies use information system access control systems that differentiate the levels of access rights for employees depending on their job duties and the level of access to classified information.
* Physical protection of servers and equipment. This is important for protection against unauthorized penetration into physical media.

**CONCLUSION**

The protection of information in law enforcement agencies is important for ensuring national security and the effectiveness of law enforcement. Various technical, organizational and legal measures are used to preserve information. The legal framework for protection is based on the Constitution of the Russian Federation, federal laws, the Criminal and Civil Codes.

There are external and internal threats to the information security of law enforcement agencies. External threats include the activities of intelligence services of other states, criminal communities, organizations that collect information about the activities of law enforcement agencies. Internal threats include violation of the regulations for the collection, processing, storage and transmission of information, failures in information systems and personnel errors.

Employee training plays a significant role in ensuring information security. Violations often occur due to errors and shortcomings in the work of personnel.

The protection of confidential information in the internal affairs bodies is not fully formed. There are nuances that prevent the further development of the data protection system from unauthorized use and distribution.

Improving the protection system will increase the effectiveness of the activities of law enforcement agencies and ensure stronger protection of society and the state from criminal and other illegal actions.

**REFERENCES**

* Beloglazov E. G. et al. Osnovy informatsionnoy bezopasnosti organov vnutrennikh del: uchebnoe posobie [Fundamentals of information security of internal affairs bodies: a textbook]. Moscow: MosU MVD Rossii, 2012.
* Information Security in the Activities of Internal Affairs Bodies of the Russian Federation: A Textbook / Ed. by Popov M. V. – M.: YUSITS "IGDI", 2017.
* Lebedev V. N. et al. Ed. by Kirin V. I. Information Protection: Textbook in 2 Parts. — Academy of Management of the Ministry of Internal Affairs of Russia, 2013.
* N. I. Zhuravlenko, V. E. Kadulin, K. K. Borzunov. Fundamentals of Information Security: A Textbook. Moscow: MosU MVD Rossii, 2012.
* Information Security Guide for Law Enforcement Agencies: A Textbook / Ed. by Smirnov A. A. – M.: YUNITI-DANA, 2020.
* Federal Law of the Russian Federation No. 149 of July 27, 2006 "On Information, Information Technologies and Information Protection".
* Decree No1233 of the Government of the Russian Federation of 03.11.94 "On the Procedure for Handling Official Information of Limited Distribution in Federal Executive Bodies".
* Federal Law of the Russian Federation No125 of 27.07.2006 "On Personal Data".
* Order of the Ministry of Internal Affairs of the Russian Federation of 24.12.2008 No1138 "On Approval of the Code of Professional Ethics of an Employee of the Internal Affairs Bodies of the Russian Federation".