**Краевой союз потребительских обществ «Крайпотребсоюз»**

**Частное профессиональное образовательное учреждение**

**«Красноярский кооперативный техникум экономики, коммерции и права»**

Курсовая работа

Тема: «Правила пользования и обращения с секретными документами и изделиями в деятельности правоохранительных органов»

 **Выполнила:** Пшык В.М.

 **Студентка гр**.: ПДА-ПДБ-2(3)

 **Проверила:** Зотина С.М.

2025

**Краевой союз потребительских обществ «Крайпотребсоюз»**

**Частное профессиональное образовательное учреждение**

**«Красноярский кооперативный техникум экономики, коммерции и права»**

|  |  |
| --- | --- |
| Согласовано:Зам. директора по практическому обучению и безопасности образовательного процесса\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.А. Каптурова«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2025 г.  | Рассмотрено:на заседании цикловой комиссии «Социально- правовых дисциплин»протокол № \_\_ от «\_\_\_\_»\_\_\_\_\_\_\_\_\_2025г.Председатель ЦК \_\_\_\_\_\_\_\_\_\_\_ Н.В. Яроцкая |
|  |  |

**Задание по курсовой работе**

*Студент* Пшык Вероника Максимовна

*Обучающийся по специальности 40.02.02* Правоохранительная деятельность

*Тема курсовой работы:* «Правила пользования и обращения с секретными документами и изделиями в деятельности правоохранительных органов»

**Содержание курсовой работы**

Введение

1.Режим секретности: понятие и принципы

* 1. Понятие режима секретности
	2. Сведения, отнесённые к государственной тайне

2. Порядок работы с секретными документами

2.1 Учет, хранение, обращение, разработка, размножение, пересылка, уничтожение секретных документов

2.2 Уровни секретности документов, как определяется уровень секретности документов. Основные положения и принципы режима секретности

Заключение

Библиографический список

###

###

**Список рекомендуемых источников:**

 1.Конституция Российской Федерации от 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования СПС: Консультант Плюс /Режим доступа:

 https://www.consultant.ru/document/cons\_LAW\_28399/

 2.Федеральный закон "О государственном оборонном заказе" от 29.12.2012 N 275-ФЗ (последняя редакция) // СПС: Консультант Плюс Режим доступа: https://www.consultant.ru/document/cons\_doc\_LAW\_140175/ (дата обращения 21.12.2023)

 3.Приказ МВД России от 30 июня 2012 года № 655 «Об утверждении Перечня документов, образующихся в деятельности органов внутренних дел Российской Федерации с указанием сроков их хранения»;

 4.Приказ МВД России от 20 августа 2010г. № 600 «Об утверждении Инструкции о порядке допуска сотрудников, федеральных государственных гражданских служащих и работников органов внутренних дел, военнослужащих и гражданского персонала внутренних войск МВД России к государственной тайне»;

 5.Приказ МВД России от 11 марта 2012г. № 015 «О мерах по обеспечению режима секретности в органах внутренних дел Российской Федерации»

 6.Указ Президента РФ от 30 ноября 1995 г. № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне» (ред. 12.10.2023) //

 7.Постановление Правительства РФ от 4 сентября 1995 г. №870 (ред. от 30.10.2021) «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» //

 8.Постановление Правительства РФ от 15.04.1995 N 333 (ред. от 03.02.2023) «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны»//

 9.Постановление Правительства РФ от 23.07.2005 N 443 (ред. от 18.03.2016) «Об утверждении правил разработки перечня сведений, отнесенных к государственной тайне»//

 10.Постановление Правительства РФ от 06.02.2010 N 63 (ред. от 29.10.2022) «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне» //

 11.Бабаков А. Л. Правовой режим временных ограничений прав военнослужащих и лиц гражданского персонала, допущенных или ранее допускавшихся к государственной тайне // Право в Вооруженных Силах. 2012. – № 9. – С. 20–24.

 12.Морозов Ю. В. Особенности допуска специальных субъектов к сведениям, составляющим государственную тайну // Журнал российского права. 2018. – № 7. – С. 123–131.

 13.Пономарева Ю.В. Категории сведений, доступ к которым может быть ограничен в режиме служебной тайны // Вестник Южно–Уральского государственного университета. Сер.: Право. – 2016. – Т. 16, № 3. – С. 116−120.

 14.Фатьянов А. А. Правовые проблемы отнесения сведений к государственной тайне в условиях модернизации экономики // Административное право и процесс. 2012. – № 7. – С. 29–32.

 15.Рыжова, О. А. Правовой режим государственной тайны / О. А. Рыжова, Д. А. Цуканова. – Текст: непосредственный // Молодой ученый. – 2020. – № 27 (317). – С. 297–301. – URL: https://moluch.ru/archive/317/72366/ (дата обращения: 29.11.2020).

 16.Шамаев В.Е. К вопросу об актуальных проблемах защиты государственной тайны // Научное и образовательное пространство: перспективы развития: материалы X Междунар. науч.–практ. конф. (Чебоксары, 9 нояб. 2018 г.) / редкол.: О.Н. Широков [и др.] – Чебоксары: ЦНС «Интерактив плюс», 2018. – С. 261–263.

 Руководитель курсовой работы \_\_\_\_\_\_\_\_\_

 С.М. Зотина

 Дата выдачи задания к курсовой работе « \_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_2025 г.

 Задание принял к исполнению \_\_\_\_\_\_\_\_\_\_\_\_В.М. Пшык

СОДЕРЖАНИЕ

 Введение……………………………………………………………………...…. 6

1.Режим секретности: понятие и принципы…………………………………10

1.1Понятие режима секретности …………………………………………….10

1.2 Сведения, отнесённые к государственной тайне………………………..11

2. Порядок работы с секретными документами…………………………….16

2.1 Учет, хранение, обращение, разработка, размножение, пересылка, уничтожение секретных документов…………………………........................16

2.2 Уровни секретности документов, как определяется уровень секретности документов. Основные положения и принципы режима секретности…….19

Заключение……………………………………………………………………..26

Библиографический список……………………………………………………27

ВВЕДЕНИЕ

Становление гражданского общества в нашей стране, достижение общественного спокойствия и социального согласия во многом связаны с утверждением правового государства. Решение этой задачи усложняется непростыми условиями продолжающегося «информационного взрыва», стремительным нарастанием информационных потоков, появлением все более оригинальных и всепроникающих информационных инфраструктур, и разведывательных технологий, которые вызывают не только позитивно – конструктивные, но и серьезные негативные социально-экономические, политические, духовно – нравственные последствия. В Российской Федерации подход к обеспечению сохранности государственной тайны более либеральный. Тем не менее, за последнее время в направлении усиления режима секретности в органах внутренних дел проделана значительная работа.

Вопросы профессиональной бдительности, сохранности государственных и служебных секретов, надежной защиты интересов страны постоянно находятся в центре внимания руководства органов внутренних дел. Указанные проблемы определяются задачами, поставленными перед министерством внутренних дел, Президентом и Правительством Российской Федерации (РФ).

В настоящее время в стране действует Доктрина информационной безопасности Российской Федерации, которая представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления информационной безопасности. Данная Доктрина принята в развитие Концепции национальной безопасности РФ применительно к информационной сфере. Все это говорит о том, что проблема защиты государственной тайны становится общегосударственной задачей и важнейшим направлением в деятельности органов внутренних дел.

Актуальность темы курсовой работы заключается в том, что государственная тайна касается всех аспектов жизни страны, а в случае нашей державы принимает характер мирового масштаба. Процветающий сегодня терроризм, сложная экономическая обстановка, возникающие изо дня в день эпидемии доселе неизвестных болезней, грозящихся перерасти в пандемии – всё это создаёт реальные угрозы, а государственная тайна содержит в себе сведения необходимые в основном для исправного функционирования государства в таких условиях. Следовательно, нужно особое внимание обращать на то, кому можно доверить государственную тайну, кто может быть допущен к разработке, хранению секретных сведений. Необходимость организации допуска как защиты информации обладает особой важностью, так как эта сфера связана не с техническими каналами или накопителями и средствами обработки информации, а непосредственно с «источниками» информации – живыми людьми от которых и зависит поддержание уровня защиты, обеспечения технических средств, циркуляции информации в глобальном смысле. Из этого вытекает роль допуска в системе защиты государственной тайны – пресечение в корне обладания секретных сведений лицами способными разгласить такую информацию или использовать её в своих целях. В этой работе будет рассмотрено понятие государственной тайны, основные положения, касающиеся системы её защиты, и в более конкретном плане допуск к сведениям, составляющим государственную тайну, организация, порядок этого допуска и документы, необходимые для его осуществления.

Объектом исследования являются правовые отношения в области ответственности сотрудников ОВД за нарушение законодательства Российской Федерации о государственной тайне.

Предметом исследования выступают нормативно – правовые акты, регламентирующие обязанности сотрудников ОВД, допущенных к работам с документами особой важности, совершенно секретными и секретными.

Целью работы является изучение обязанностей сотрудников ОВД, допущенных к работам с документами особой важности, совершенно секретными и секретными.

Для достижения указанной цели поставлены следующие задачи:

* рассмотреть понятие «режима секретности»;
* проанализировать сведения, отнесенные к государственной тайне;
* раскрыть основные положения и принципы режима секретности;
* ознакомиться с грифами секретности;
* определить принципы засекречивания и рассекречивания информации, составляющей государственную тайну;
* изучить обязанности сотрудников ОВД, допущенных к работам с документами особой важности, совершенно секретными и секретными.

Методологическую основу исследования составили: системный подход к данной теме, а также сбор тематической информации, изучение первичных документов, анализ текста нормативно-правовых актов.

Теоретической базой исследования являются работы авторов, таких как М.Н. Басаков, О.П. Говорухин, А.А. Дворников, О.И. Замыцкова, А.В. Заряев и другие.

Нормативную базу исследования составили: Конституция Российской Федерации, Постановление Правительства РФ «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности», Постановление Правительства Российской Федерации «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне», Федеральный закон «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации», Федеральный закон «Об информации, информационных технологиях и о защите информации», Федеральный закона «Об оперативно-розыскной деятельности», Федеральный закон РФ «О государственной тайне», Постановление Правительства РФ «Об утверждении Положения о порядке допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов к государственной тайне», ГОСТ Р 50922-2006 «Защита информации».

Работа состоит из введения, двух глав, заключения и списка используемых источников.

Во введении обосновывается актуальность темы курсовой работы, формулируются цели и задачи, определяется объект предмет, методологическая основа, теоретическая и нормативная база.

В первой главе рассматривается режим секретности: понятия и признаки.

Вторая глава посвящена обязанностям сотрудников ОВД, допущенных к работам с документами особой важности, совершенно секретными, секретными.

В заключении содержатся выводы по проведенному исследованию в курсовой работе.

1 Режим секретности: понятие и принципы

* 1. Понятие режима секретности

Понятие «режим секретности» представляет собой комплекс организационных, технических и иных мероприятий, направленных на обеспечение сохранения в тайне сведений, составляющих государственную

тайну и включающих в себя:

* порядок и правила разработки, учета, хранения, размножения, доставки, обращения, уничтожения материальных носителей информации;
* проведение совещаний по секретным вопросам;
* технические меры защиты;
* мероприятия по допуску;
* обучение и воспитание личного состава;
* контроль за соблюдением установленных правил;
* поиск возможных каналов утечки информации.

Тайна – это понятие, имеющее несколько смысловых значений. В повседневном обиходе, на бытовом уровне понятие тайна трактуется как нечто неразгаданное, скрытое от посторонних глаз, как вещь в себе. Применительно к органам государственной власти и управления под тайной понимается то, что осознанно скрывается от других, что известно строго определенному кругу лиц. Иначе говоря, тайну составляют те сведения, которые не подлежат разглашению. Такие сведения содержатся в секрете, как правило, определенное время, обусловленное их государственной или служебной значимостью, необходимостью, вытекающей из интересов страны в целом или отдельного ведомства (министерства, администрации, департамента, управления, представительного или судебного органа власти). Лишь после того, как необходимость сохранения в тайне каких-то сведений отпадает, они могут быть оглашены либо опубликованы. Вообще же всегда следует помнить, что степень ценности информации и необходимая степень надежности ее защиты находятся в прямой зависимости.

1.2 Сведения, отнесенные к государственной тайне

Государственная тайна – защищаемые государством сведения в области

его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности (ОРД), распространение которых может нанести ущерб безопасности Российской

Федерации.

Носители сведений, составляющих государственную тайну, – материальные объекты, в том числе физические поля, в которых сведения,

составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов. Доступ к сведениям, составляющим государственную тайну, – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну.

Система защиты государственной тайны – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях. Источники конфиденциальной информации – обладатель (носитель) охраняемых сведений, представляющих интерес для противника (преступников). Сюда относятся: люди; документы; публикации; технические носители; технические средства обеспечения служебной деятельности; специзделия; отходы управленческой деятельности.

На сегодняшний день система защиты государственной тайны в органах внутренних дел должна отвечать следующим принципам:

* принцип ограничения доступа к информации и их носителям. Значение этого принципа очевидно. Основные методы его реализации – это семантические (криптографические) методы ограничения доступа к большей части информации и физические методы ограничения доступа к критическим информационным ресурсам (к зонам хранения ключевой информации, используемой в криптографических методах; к зонам, где обработка информации возможна только в открытом виде).
* принцип минимальной ценности информации. Он предписывает создавать информационные системы с наименьшим количеством секретной или конфиденциальной информации. В идеальном варианте основная масса информации должна иметь самый низкий статус безопасности и возможность пользования ею только в случае поступления запроса
* принцип персональной ответственности исполнителей или владельцев информации. Выполнение этого принципа позволяет снизить вероятность угроз безопасности информации от несанкционированного доступа со стороны внутренних субъектов.
* принцип тотальной, сквозной идентификации информационных пользователей. Этот принцип определяет необходимость наличия уникальных идентификаторов пользователей у всех информационных систем.
* принцип взаимного установления подлинности информационного пользователя. Основным направлением распространения данного принципа является применение криптографических методов аутентификации, активизированных в рамках информационного процесса.
* принцип функциональной полноты системы защиты информации. Этот принцип определяет необходимость наличия у информационной системы определенных функций защиты (например, функций идентификации, аутентификации, физической защиты или шифрования). Все эти принципы должны учитываться при разработке и создании защищенных информационных технологий и систем в ОВД.

Проанализируем сведения, отнесенные к государственной тайне и находящиеся в введении МВД России.

Сведения в военной области:

* сведения, раскрывающие планы применения войск, оперативные планы, документы боевого управления, документы по приведению войск в различные степени готовности;
* сведения, раскрывающие состояние оперативной подготовки войск, состав и состояние систем управления;
* сведения о мобилизационном развертывании войск; сведения, раскрывающие долгосрочные прогнозы развития вооружения и военной техники, содержание или результаты выполнения целевых программ;
* сведения, обеспечивающие безопасность объектов ядерного комплекса; сведения, раскрывающие дислокацию, организационную структуру, вооружение, не подлежащие открытому объявлению в соответствии с международными обязательствами Российской Федерации;
* сведения о дислокации, назначении, степени готовности или защищенности режимных объектов;
* сведения, раскрывающие распределение или использование полос радиочастот радиоэлектронными средствами военного или специального назначения;
* сведения, раскрывающие организацию или функционирование всех видов связи.

Сведения в области экономики, науки и техники:

* сведения о показателях, определяющих подготовку экономики Российской Федерации к устойчивому функционированию в военное время;
* сведения, раскрывающие затраты на научно-исследовательские, опытно-конструкторские работы по созданию вооружения и военной техники;
* сведения о способах, обеспечивающих защиту банкнот от подделок, а также способах определения их подлинности.

Сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности:

* сведения, раскрывающие организацию или фактическое состояние защиты государственной тайны;
* сведения, раскрывающие силы, средства, методы, планы и результаты оперативно-розыскной деятельности.
* сведения о лицах, сотрудничавших на конфиденциальной основе с органами, осуществляющими оперативно-розыскную деятельность;
* сведения, раскрывающие принадлежность конкретных лиц к подразделениям по борьбе с организованной преступностью;
* сведения, раскрывающие силы, средства и методы ведения следствия по уголовным делам о государственных преступлениях

Перечисленные сведения охраняются государством и могут быть рассекречены только на основании постановления руководителя органа, осуществляющего оперативно-розыскную деятельность. Кроме того, государственную тайну составляют сведения, раскрывающие принадлежность конкретных лиц к подразделениям по борьбе с организованной преступностью, проводимые ими оперативно-поисковые и оперативно-технические мероприятия, деятельность органов радиоэлектронной разведки средств связи.

В ст. 12 Федерального закона РФ «Об оперативно-розыскной деятельности» [3] перечислены категории сведений, составляющих государственную тайну. К ним относятся сведения:

* об организации и тактике проведения оперативно-розыскных мероприятий;
* об используемых при проведении негласных оперативно-розыскных мероприятий силах, средствах, источниках, методах, планах и результатах оперативно-розыскной работы;
* о лицах, внедренных в организованные преступные группы, о штатных негласных сотрудниках органов, осуществляющих оперативно-розыскную деятельность, а также о лицах, оказывающих им содействие на конфиденциальной основе.

Перечисленные сведения охраняются государством и могут быть рассекречены только на основании постановления руководителя органа, осуществляющего оперативно-розыскную деятельность. Кроме того, государственную тайну составляют сведения, раскрывающие принадлежность конкретных лиц к подразделениям по борьбе с организованной преступностью, проводимые ими оперативно-поисковые и оперативно-технические мероприятия, деятельность органов радиоэлектронной разведки средств связи.

2.Порядок работы с секретными документами

2.1 Учет, хранение, обращение, разработка, размножение, пересылка, уничтожение секретных документов

Учет секретных документов – это регистрация и контроль за их сохранностью. В практической деятельности органов внутренних дел существует две формы учета секретных документов: журнальная и карточная.

При журнальной системе учета информация о секретных документах хранится в специальных журналах. При карточной системе учета информация хранится на специальных карточках, отдельно для каждого секретного документа.

При учете секретных документов присваиваются регистрационные номера и фиксируется следующая информация:

-гриф;

- количество листов;

- количество экземпляров;

- источник поступления;

- краткое содержание;

- дата поступления.

Учету подлежат:

- секретные документы;

- рабочие тетради;

- специальные блокноты;

- отдельные листы бумаги.

Хранение секретных документов – это установленный порядок, обеспечивающий содержание в безопасности секретных документов на рабочих местах и в специальных хранилищах, а также порядок, предотвращающий порчу секретных документов, их утрату и несанкционированное копирование.

В рабочее время секретные документы хранятся у исполнителей в личных сейфах или в секретных портфелях (папках). После окончания работы секретные документы сдаются на хранение в режимно-секретные подразделения.

 При обращении с секретными документами следует соблюдать следующие правила:

- секретные документы выдаются только под личную роспись;

-работа с секретными документами осуществляется в специальных помещениях;

-при работе с секретными документами на рабочем столе должны находиться только необходимые в данный момент документы;

-запрещается держать секретные документы вместе с несекретными;

- запрещается хранить секретные документы в рабочих столах;

-при приеме посетителей нельзя оставлять секретные документы в положении, удобном для обозрения;

-необходимо убирать секретные документы в сейф при временном выходе из помещения;

-запрещается выносить секретные документы за пределы охраняемой территории;

-при окончании работы с секретными документами необходимо проверить наличие всех секретных документов;

-секретные документы разрабатываются только в специальных блокнотах, рабочих тетрадях;

-степень секретности документа определяется в соответствии с перечнями;

- количество экземпляров секретных документов определяется служебной необходимостью;

-в секретных документах должен быть представлен минимально возможный объем секретных сведений;

-запрещается снимать копии с секретных документов без разрешения;

-запрещается самостоятельно уничтожать секретные документы.

 Порядок оформления секретных документов:

Гриф;

N экземпляра;

Адрес;

Текст;

Приложения;

Подпись;

Порядок оформления последнего листа:

Исполнители;

Гриф;

Количество листов и экземпляров;

адреса экземпляров;

Машинистка;

Дата.

 Размножение секретных документов. Подготовленный секретный документ подается исполнителями для размножения в 1-й отдел РСО.

Сдаются только те листы секретных документов, которые подлежат копированию. После размножения исполнитель получает документы и расписывается за оригинал и за каждую копию. Не подлежат копированию секретные документы с грифом «особой важности».

 Секретные документы пересылаются только через РСО предприятия. Полностью оформленный и подписанный секретный документ сдается исполнителем в 1-й отдел для пересылки.

Перед отправкой секретный документ помещается в специальную упаковку, исключающую несанкционированное изъятие секретных документов.

Пересылка секретных документов в другие города осуществляется подразделениями специальной связи Министерства Связи РФ и подразделениями фельдегерской связи МО РФ. При пересылке в рамках одного города используются: курьеры, нарочные, работники РСО, исполнители.

Лица, занятые доставкой секретной почты обеспечиваются служебным транспортом и охраной. Передача секретных документов адресатам осуществляется по разносным книгам, распискам, реестрам под личную роспись принимающего, которая скрепляется печатью 1-го отдела с проставлением времени и числа.

 Уничтожение секретных документов. Секретные документы, потерявшие свою практическую и другую ценность, подлежат уничтожению. Для уничтожения секретных документов приказом руководителя предприятия назначается комиссия в составе не менее 3-х человек.

Порядок работы комиссии:

1) оценка ценности секретных документов;

2) написание акта на уничтожение секретных документов;

3) проведение сверки представленных на уничтожение документов с записями в журналах и карточках учета;

4) проставление росписей в акте и представление его на утверждение руководителю предприятия;

5) уничтожение в присутствии членов комиссии.

Акт на уничтожение хранится в 1-м отделе.

2.2 Уровни секретности документов, как определяется уровень секретности документов. Основные положения и принципы режима секретности

Уровни секретности документов Подробная информация о документации с грифом «Секретно» прописывается в Законе РФ от 21 июля 1993 г. N 5485-I «О государственной тайне». Согласно данному закону, бумаги, которые содержат государственную тайну и подлежат охране, могут относиться к одному из

содержится государственная тайна. Порядок работы с информацией в таких документах четко определяется действующим законодательством.

3. Уровень секретности «Для служебного пользования». Нельзя назвать такой гриф статусом секретности, однако в данном случае доступ к служебной информации разрешается исключительно сотрудникам компании. Использовать ее бесконтрольно запрещено. Государственной тайной является информация в военной сфере, а также в областях экономики, науки, техники, внешней политики, разведки и противодействия терроризму. Засекречиванием носителя должны заниматься эксперты, от квалификации которых и знаний законодательства напрямую зависит сохранность тайных сведений. Контроль над установкой уровня секретности документа производится должностным лицом, которое подписывало бумагу. Оно наряду с исполнителем является ответственным за верное присвоение документации грифа секретности. В случае присутствия в документе данных разного уровня секретности он получает гриф по высшей степени среди них.

Как определяется уровень секретности документов: основные правила Грамотно решить задачу по установке грифа секретности и сохранения государственной тайны можно лишь при системном подходе к ней. Поэтому следует опираться на ряд правил. Необходимо не допускать самовольства в данной сфере, в противном случае не избежать проблем в работе с документацией или с утечкой важной информацией.

Перечислим правила, о которых идет речь.

1. Правило системного подхода к определению уровня секретности документов. Основная суть этого принципа – это учет общей проблемы засекречивания. Нужно принимать во внимание существующую двойственность: с одной стороны, есть цель к обеспечению надежной сохранности государственной тайны, с другой – нельзя необоснованно и массово засекречивать данные. А потому недопустимо как завышение грифа секретности, так и занижение. Следует избегать любых крайностей.

 2. Правило объективности при присвоении грифа секретности. Существует Перечень сведений, подлежащих засекречиванию, на который и нужно опираться в работе. Субъективный подход недопустим.

3. Правило оптимизации объема секретных данных в бумагах. В отдельной документации секретные сведения должны содержаться по минимуму и строго в необходимом для решения рассматриваемого вопроса объеме.

 4. Правило периодического пересмотра уровня секретности документов. Со временем степень секретности может снизиться или вообще утратиться. Потому и возникает необходимость рано или поздно пересмотреть ее.

Основные положения и принципы режима секретности

 Система защиты государственной тайны в общем виде представляет собой совокупность мер, направленных на противодействие иностранным разведкам, снижение рисков утечки и разглашения секретных сведений через информационные системы и кадры, ведение учета и контроля за выполнением требований нормативных документов, регулирующих режим секретности. Режим секретности создается по единым правилам для всех госорганов, организаций и ведомственных учреждений.

Основные регулирующие документы:

* Закон РФ «О государственной тайне»; [6]
* Инструкция по обеспечению режима секретности в Российской Федерации» (утв. Постановлением Правительства РФ № 3-1 от 5 января 2004 г.); [6]
* Инструкция о порядке допуска должностных лиц и граждан Российской Федерации» (постановление Правительства РФ от 06.02.2010г. № 63); [5]
* «Положение о лицензировании предприятий для работы с государственной тайной» (утв. Постановления Правительства РФ от 15 апреля 1995 года № 333). [4]

В систему защиты государственной тайны входит:

* допускная работа. Оформление допуска к гостайне на руководителя фирмы и сотрудников, которые будут непосредственно работать с секретными сведениями. Ведение учета документов и лиц, допущенных к госта (составление документов о допуске и доступе к государственной тайне, поддержание их в актуальном виде, выдача соответствующих справок, разрешение для выезда за границу);
* организация пропускного режима на предприятии. Например, это не только турникеты и проверка документов при входе в помещение, но и создание зон ограниченного доступа только для лиц, имеющих допуск к государственной тайне. Особенно актуально на оборонных предприятиях и заводах, конструкторских бюро и прочих организациях, где наряду с государственной тайной идет работа с другой информацией;
* создание защищенных технических каналов обмена и обработки информации. Сюда входит предоставление создание или предоставление автоматизированного рабочего места, оснащенного специальным сертифицированным оборудованием и средствами защиты информации, обработка и отправка секретных документов по защищенным каналам связи, предоставление выделенных помещений для секретных переговоров, периодическая проверка помещений и оборудования на наличие средств несанкционированного получения информации;
* работа с персоналом. Сюда помимо допускной работы и ведение номенклатуры должностей входят инструктажи по обеспечению информационной безопасности и защите государственной тайны, выплата надбавок за секретность, контроль за тем, как исполняются требования инструкций и локальных актов, выявление и расследование всех случаев несоблюдения должностных обязанностей по соблюдению режима секретности.

Основные принципы обеспечения действенного режима секретности в системе государственной службы. Этот принцип детерминируется тем, что вся служебная информация в системе государственной службы является государственной собственностью. Управлять и распоряжаться ею может только государство.

Принцип конспирации означает необходимость и легитимность использования в процессе ОРД правил и приемов, позволяющих сохранять в тайне действия правоохранительных органов по их разоблачению. Требование сохранения в тайне действий правоохранительных органов обусловливается рядом обстоятельств, а именно:

* потребностью принятия адекватных мер борьбы с преступлениями, которые готовятся и совершаются в условиях повышенных мер предосторожности с целью избежать уголовного наказания;
* когда оперативно-розыскные мероприятия проводятся при наличии непроверенной информации. Здесь конспиративность помогает избежать необоснованной компрометации лиц, подозреваемых в совершении преступлений;
* сохранением конфиденциальных сведений, которые в основном являются условием оказания гражданами помощи в раскрытии преступлений, гарантией сохранения им здоровья и жизни

Принцип конспирации находит отражение в ряде статей Федерального закона «Об оперативно-розыскной деятельности», которые регламентируют правила и приемы действий оперативных сотрудников, позволяющие сохранять их в тайне. К ним относятся:

* определение перечня сведений об оперативно-розыскной деятельности, составляющих государственную тайну;
* ограничение пределов оперативно-розыскной информации, предоставляемой по требованию лица на основании запросов;
* обязанность оперативных подразделений соблюдать правила конспирации при проведении оперативно-розыскных мероприятий;
* ограничение судей в праве получения сведений о лицах, оказывающих содействие правоохранительным органам на конфиденциальной основе;
* требование создания условий по защите сведений, содержащихся в предоставляемых судье оперативно-служебных документах;
* обязательное использование документов, зашифровывающих личность и ведомственную принадлежность предприятий, помещений и транспортных средств;
* право на создание легендированных предприятий и организаций.

Существующая ныне система защиты государственной тайны не может в полном объеме обеспечить эффективную защиту необходимого количества сведений. Согласно исследованиям, проведенным по этой теме, первым и основным аспектом совершенствования системы защиты государственной тайны в ОВД является коренное изменение отношения всех работников органов внутренних дел к проблеме защиты информации. В научных работах 16 отмечается, что тот сложившийся десятилетиями стереотип, когда секретные сведения ОВД воспринимались как нечто несущественное, слабо интересующее спецслужбы вероятного противника, к сожалению, сохранился и до сих пор. Теперь становится очевидным, что оперативные материалы имеющиеся в распоряжении ОВД, могут эффективно использоваться в политической борьбе, а, следовательно, могут оказать ощутимое влияние на ход общественно-политической жизни страны. И наконец, организованные преступные группировки и связанные с ними коррумпированные служащие государственного аппарата обладают куда большими возможностями по добыванию закрытой информации ОВД, чем преступная среда десятилетней давности. Помимо этого, информация стала дорогостоящим и желанным товаром, а ОВД имеют возможность и получают представляющую в том числе и коммерческий интерес информацию о деятельности различных предприятий и организаций. Проанализируем наиболее значимые государственные правовые документы, регламентирующие соблюдение режима секретности. 21 июля 1993 г. был принят Закон РФ «О государственной тайне», который регулирует правоотношения, связанные с отнесением информации к государственной тайне. Он также устанавливает единые требования по охране секретов в органах государственной власти и управления, на предприятиях, в учреждениях и организациях, предусматривает введение в перспективе нового государственного ведомства – Центрального органа управления системой охраны государственной тайны, общее руководство и контроль за работой которого предполагается возложить на Президента и Правительство страны.

ЗАКЛЮЧЕНИЕ

В курсовой работе мы рассмотрели, какие существуют грифы секретности документов, а также принципы определения секретности и отнесения их к нужным грифам. Так мы смогли выделить для себя три основным грифа: секретно, совершенно секретно и особой важности. Так же мы узнали, что собой представляет степень секретности. Таким образом мы вывели общее понятие, что показатель степени секретности документов Отнесены к государственной тайне и засекречены могут быть названные в законе сведения в военной области, о внешней политике, экономике, научно-исследовательских и проектных работах, технологиях, имеющих важное оборонное или экономическое значение, о разведывательной, контрразведывательной, оперативно-розыскной деятельности. Срок засекречивания сведений, составляющих государственную тайну, не должен превышать 30 лет. В исключительных случаях этот срок может быть продлен по заключению межведомственной комиссии по защите государственной тайны.

Разглашение государственной тайны – это предание огласке сведений, составляющих государственную тайну, в результате чего эти сведения становятся достоянием лиц, не имеющих к ним доступа.

По ходу проведенного исследования по данной теме был сделан следующий вывод.

Допуск к сведениям, составляющим государственную тайну, является первейшей мерой по обеспечению защиты информации, и его надежность в значительной мере может предупредить и пресечь утечку информации через неблагонадёжных граждан и должностных лиц.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

 1.Конституция Российской Федерации от 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования СПС: Консультант Плюс /Режим доступа:

 https://www.consultant.ru/document/cons\_LAW\_28399/

 2.Федеральный закон "О государственном оборонном заказе" от 29.12.2012 N 275-ФЗ (последняя редакция) // СПС: Консультант Плюс Режим доступа: https://www.consultant.ru/document/cons\_doc\_LAW\_140175/ (дата обращения 21.12.2023)

 3.Приказ МВД России от 30 июня 2012 года № 655 «Об утверждении Перечня документов, образующихся в деятельности органов внутренних дел Российской Федерации с указанием сроков их хранения»;

 4.Приказ МВД России от 20 августа 2010г. № 600 «Об утверждении Инструкции о порядке допуска сотрудников, федеральных государственных гражданских служащих и работников органов внутренних дел, военнослужащих и гражданского персонала внутренних войск МВД России к государственной тайне»;

 5.Приказ МВД России от 11 марта 2012г. № 015 «О мерах по обеспечению режима секретности в органах внутренних дел Российской Федерации»

 6.Указ Президента РФ от 30 ноября 1995 г. № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне» (ред. 12.10.2023) //

 7.Постановление Правительства РФ от 4 сентября 1995 г. №870 (ред. от 30.10.2021) «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» //

 8.Постановление Правительства РФ от 15.04.1995 N 333 (ред. от 03.02.2023) «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны»//

 9.Постановление Правительства РФ от 23.07.2005 N 443 (ред. от 18.03.2016) «Об утверждении правил разработки перечня сведений, отнесенных к государственной тайне»//

 10.Постановление Правительства РФ от 06.02.2010 N 63 (ред. от 29.10.2022) «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне» //

 11.Бабаков А. Л. Правовой режим временных ограничений прав военнослужащих и лиц гражданского персонала, допущенных или ранее допускавшихся к государственной тайне // Право в Вооруженных Силах. 2012. – № 9. – С. 20–24.

 12.Морозов Ю. В. Особенности допуска специальных субъектов к сведениям, составляющим государственную тайну // Журнал российского права. 2018. – № 7. – С. 123–131.

 13.Пономарева Ю.В. Категории сведений, доступ к которым может быть ограничен в режиме служебной тайны // Вестник Южно–Уральского государственного университета. Сер.: Право. – 2016. – Т. 16, № 3. – С. 116−120.

 14.Фатьянов А. А. Правовые проблемы отнесения сведений к государственной тайне в условиях модернизации экономики // Административное право и процесс. 2012. – № 7. – С. 29–32.

 15.Рыжова, О. А. Правовой режим государственной тайны / О. А. Рыжова, Д. А. Цуканова. – Текст : непосредственный // Молодой ученый. – 2020. – № 27 (317). – С. 297–301. – URL: https://moluch.ru/archive/317/72366/ (дата обращения: 29.11.2020).

 16.Шамаев В.Е. К вопросу об актуальных проблемах защиты государственной тайны // Научное и образовательное пространство: перспективы развития : материалы X Междунар. науч.–практ. конф. (Чебоксары, 9 нояб. 2018 г.) / редкол.: О.Н. Широков [и др.] – Чебоксары: ЦНС «Интерактив плюс», 2018. – С. 261–263.

**Private professional educational institution**

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

Interdisciplinary educational project in the disciplines "Paperwork and secrecy regime" and "English language"

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

**Completed by**: student of the group

 PDA-2(3)

 **Specialty**: Law enforcement

 Pshyk Veronika Maksimovna

 **Project leader**: teacher highest

 qualification category

 Panasyuk Tatiana Vladimirovna

2025

**Content**

Annotation………………………………………………………………………….3

Introduction...............................................................................................................4

1 Secrecy regime: concept and principles………………………………………….6

* 1. The concept of secrecy…………………………………………………………6
	2. Information classified as a State secret…………………………………………7
1. How to handle classified documents………………………………………...…9
	1. Accounting, keeping, conversion, development, reproduction, forwarding, destruction of secret documents………………………………………………..9

Conclusion ………………………………………………………………………..10

List of sources used……………………………………………………………….11

**Annotation**

The research topic is devoted to the Rules of use and handling of classified documents and products in the activities of law enforcement agencies. This paper discusses the rules for the use and handling of classified documents and products in the activities of law enforcement agencies. Special attention is paid to legislative and regulatory acts regulating the protection of state secrets, as well as internal regulations ensuring information security.

The basic principles of working with classified materials are analyzed, including their classification, storage procedure, accounting, handling, reproduction, transfer and destruction. Measures to prevent information leaks are being discussed. The paper also examines current challenges and threats related to the handling of classified documents in the context of digitalization and globalization, as well as recommendations for improving the level of protection of confidential information in law.

**Keywords:**

Secret documents, levels of secrecy, destruction of secret documents, observance of the secrecy regime, secrecy stamps, state secret, principles of secrecy, reproduction of secret documents, rules for handling secret documents, secrecy, duties of internal affairs officers.

**Introduction**

**Relevance of the project:** a state secret concerns all aspects of the country's life, and in the case of our country, it takes on a global scale. Terrorism, which is flourishing today, the difficult economic situation, and epidemics of hitherto unknown diseases that threaten to develop into pandemics, all pose real threats, and state secrets contain information that is mainly necessary for the proper functioning of the state in such conditions. Therefore, special attention should be paid to who can be entrusted with state secrets, who can be allowed to develop and store classified information.

**The problem of the project:** special attention should be paid to who can be entrusted with state secrets, who can be allowed to develop and store classified information. The need to organize access as information protection is of particular importance, since this area is not related to technical channels or storage devices and information processing facilities, but directly to the "sources" of information – living people on whom it depends to maintain the level of protection, provision of technical means, and information circulation in a global sense.

**The purpose of the project:** the study of the duties of employees of the Department of Internal Affairs, who are allowed to work with documents of special importance, top secret and secret.

**Tasks:**

1. Consider the concept of a "secrecy regime";

2. Analyze information classified as a state secret;

3. To reveal the main provisions and principles of the secrecy regime;

4. Get acquainted with the secrecy labels;

5. Determine the principles of classifying and declassifying information constituting a state secret;

6. To study the duties of employees of the Department of Internal Affairs who are allowed to work with documents of special importance, top secret and secret.

**Hypothesis:** The introduction of strict and clear rules for the use of classified documents in law enforcement agencies increases the level of security of government data.

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

**1 Secrecy regime: concept and principles**

* 1. **The concept of the secrecy regime**

The concept of "secrecy regime" is a set of organizational, technical and other measures aimed at ensuring the secrecy of information constituting a state

secret and including:

* The procedure and rules for the development, accounting, storage, reproduction, delivery, handling, and destruction of tangible media;
* holding meetings on classified issues;
* technical protection measures;
* admission arrangements;
* training and education of personnel;
* monitoring compliance with established rules;
* search for possible information leakage channels.

A secret is a concept that has several semantic meanings. In everyday use, at the household level, the concept of mystery is interpreted as something unsolved, hidden from prying eyes, as a thing in itself. In relation to public authorities and management, secrecy refers to what is deliberately hidden from others, which is known to a strictly defined circle of people. In other words, the information that is not subject to disclosure is a secret. Such information is kept secret, as a rule, for a certain time, due to their state or official significance, necessity arising from the interests of the country as a whole or a separate department (ministry, administration, department, management, representative or judicial authority). Only after the need to keep some information secret disappears, it can be announced or published. In general, it should always be remembered that the degree of value of information and the necessary degree of reliability of its protection are directly related.

**1.2 Information classified as a State secret**

Today, the system of protecting state secrets in the internal affairs bodies must comply with the following principles:

- the principle of restricting access to information and its media. The significance of this principle is obvious. The main methods of its implementation are semantic (cryptographic) methods of restricting access to most information and physical methods of restricting access to critical information resources (to areas where key information used in cryptographic methods is stored; to areas where information processing is possible only in clear text).

- the principle of the minimum value of information. It prescribes the creation of information systems with the least amount of secret or confidential information. Ideally, the bulk of the information should have the lowest security status and be usable only if requested.

- the principle of the minimum value of information. It prescribes the creation of information systems with the least amount of secret or confidential information. Ideally, the bulk of the information should have the lowest security status and be usable only if requested.

- the principle of personal responsibility of performers or owners of information. The implementation of this principle makes it possible to reduce the likelihood of threats to information security from unauthorized access by internal actors.

The principle of total, end-to-end identification of information users. This principle determines the need for all information systems to have unique user identifiers.

- the principle of mutual authentication of the information user. The main focus of this principle is the use of cryptographic authentication methods activated as part of the information process.

-the principle of functional completeness of the information security system. This principle determines the need for an information system to have certain security functions (for example, identification, authentication, physical protection, or encryption functions). All these principles should be taken into account when developing and creating secure information technologies and systems in the Department of Internal Affairs.

The information is protected by the state and can be declassified only on the basis of a resolution of the head of the body carrying out operational investigative activities. In addition, information disclosing the affiliation of specific individuals to units for combating organized crime, their operational search and operational technical measures, and the activities of electronic intelligence agencies of communications facilities constitute a State secret.

**2 How to work with classified documents**

**2.1 Accounting, storage, handling, development, reproduction, transfer, destruction of classified documents**

Accounting for secret documents is the registration and control of their safety. In the practice of law enforcement agencies, there are two forms of accounting for classified documents: journal and card records.

The storage of secret documents is an established procedure that ensures the security of secret documents at workplaces and in special vaults, as well as an order that prevents damage to secret documents, their loss and unauthorized copying.

Destruction of classified documents. Secret documents that have lost their practical and other value must be destroyed. By order of the head of the enterprise, a commission consisting of at least 3 people is appointed to destroy secret documents.

Reproduction of secret documents. The prepared secret document is submitted by the performers for reproduction to the 1st department of the RSO.

Only those sheets of secret documents that must be copied are submitted. After reproduction, the performer receives the documents and signs for the original and for each copy. Classified documents marked with "special importance" are not subject to copying.

Persons engaged in the delivery of secret mail are provided with official transport and security. The transfer of secret documents to the addressees is carried out according to the delivery books, receipts, registers under the personal signature of the recipient, which is sealed with the seal of the 1st department with the time and date affixed.

**Conclusion**

In the course work, we looked at what types of classified documents exist, as well as the principles of determining secrecy and assigning them to the right categories. So we were able to identify three main categories for ourselves: secret, top secret and of special importance. We also found out what the degree of secrecy is. Thus, we have deduced the general concept that the indicator of the degree of secrecy of documents is classified as a state secret and the information mentioned in the law in the military field, on foreign policy, economics, research and design work, technologies of important defense or economic importance, on intelligence, counterintelligence, operational and investigative activities can be classified. The period of secrecy of information constituting a state secret should not exceed 30 years. In exceptional cases, this period may be extended by the conclusion of the interdepartmental commission for the protection of State secrets.

Disclosure of a state secret is the disclosure of information that constitutes a state secret, as a result of which this information becomes the property of persons who do not have access to it.

In the course of the conducted research on this topic, the following conclusion was made.

Access to information constituting a state secret is the first measure to ensure information protection, and its reliability can significantly prevent and stop information leakage through unreliable citizens and officials.

**List of sources used**

1. The Constitution of the Russian Federation of 12.12.1993 with amendments approved during the all-Russian vote of the ATP: Consultant Plus /Access mode:

https://www.consultant.ru/document/cons\_LAW\_28399 /

2.Federal Law "On the State Defense Order" dated December 29, 2012 N 275-FZ (latest edition) // SPS: Consultant Plus Access mode: https://www.consultant.ru/document/cons\_doc\_LAW\_140175 / (accessed 12/21/2023

3. Order of the Ministry of Internal Affairs of Russia dated June 30, 2012 No. 655 "On Approval of the List of Documents Generated in the Activities of the Internal Affairs bodies of the Russian Federation with an Indication of their retention periods";

 4. Order of the Ministry of Internal Affairs of Russia dated August 20, 2010 No. 600 "On Approval of Instructions on the Procedure for Access to State Secrets for Employees, Federal Government Civil Servants and Employees of Internal Affairs Bodies, military personnel and civilian personnel of the Internal Troops of the Ministry of Internal Affairs of Russia";

5. Order of the Ministry of Internal Affairs of the Russian Federation No. 015 dated March 11, 2012 "On Measures to ensure Secrecy in the Internal Affairs Bodies of the Russian Federation"

6. Decree of the President of the Russian Federation No. 1203 dated November 30, 1995 "On Approval of the List of Information Classified as a State Secret" (as amended on 10/12/2023) //

 7. Decree of the Government of the Russian Federation of September 4, 1995 No. 870 (as amended on 10/30/2021) "On Approval of the Rules for Classifying Information Constituting a State Secret to various Degrees of secrecy" //

 8. Decree of the Government of the Russian Federation No. 333 dated 04/15/1995 (as amended on 02/03/2023) "On Licensing the activities of enterprises, institutions and organizations involved in the use of Information Constituting a State Secret, the creation of information Protection tools, as well as the implementation of measures and (or) the provision of services for the protection of State secrets"//

9. Decree of the Government of the Russian Federation No. 443 dated 07/23/2005 (as amended on 03/18/2016) "On Approval of the Rules for Developing a List of Information Classified as a State Secret"//

10. Decree of the Government of the Russian Federation No. 63 dated 02/06/2010 (as amended on 10/29/2022) "On Approval of Instructions on the Procedure for Admitting Officials and Citizens of the Russian Federation to State Secrets"

11. Babakov A. L. The legal regime of temporary restrictions on the rights of military personnel and civilian personnel admitted or previously admitted to state secrets // Law in the Armed Forces. 2012. No. 9. pp. 20-24.

12.Morozov Yu. V. Features of access of special subjects to information constituting a state secret // Journal of Russian Law. 2018. No. 7. pp. 123-131.

13.Ponomareva Yu.V. Categories of information, access to which may be restricted in the regime of official secrecy // Bulletin of the South Ural State University. Ser.: Pravo, 2016, vol. 16, No. 3, pp. 116-120.

14. Fatyanov A. A. Legal problems of classifying information as a state secret in the context of economic modernization // Administrative Law and Process, 2012, No. 7, pp. 29-32.

 15.Ryzhova, O. A. The legal regime of state secrets / O. A. Ryzhova, D. A. Tsukanova. – Text : direct // Young scientist. – 2020. – № 27 (317). – Pp. 297-301. – URL: https://moluch.ru/archive/317/72366 / (date of reference: 11/29/2020).

16.Shamaev V.E. On the issue of urgent problems of protecting state secrets // Scientific and educational space: development prospects : proceedings of the X International Scientific and Practical Conference (Cheboksary, November 9, 2018) / editor: O.N. Shirokov [et al.] – Cheboksary: CNS "Interactive Plus", 2018. – pp. 261-263.