Новоуренгойский филиал Профессионального образовательного учреждения «Уральский региональный колледж»

КУРСОВАЯ РАБОТА

ПРИЕМ ВХОДЯЩИХ СЕКРЕТНЫХ ДОКУМЕНТОВ.

УЧЕТ СЕКРЕТЫХ ДОКУМЕНТОВ

МДК 01.05 ДЕЛОПРОИЗВОДСТВО И РЕЖИМ СЕКРЕТНОСТИ

40.02.02 Правоохранительная деятельность

Обучающегося гр. ПД-278 \_\_\_\_\_\_\_\_\_ Санду Ана-Мария

\_\_.05.2020

Оценка за выполнение и защиту курсовой работы \_\_\_\_\_\_\_\_\_\_\_\_

Проверил \_\_\_\_\_\_\_\_\_\_ Абрамович Анастасия Владимировна

\_\_.05.2020

Новый Уренгой, 2020

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 3 ГЛАВА 1. ПОНЯТИЕ О КОНФИДЕНЦИАЛЬНОСТИ, СВЕДЕНИЯ КОММЕРЧЕСКОЙ ТАЙНЫ И СОДЕРЖАНИЕ ГОСУДАРСТВЕННОЙ ТАЙНЫ

1.1 Понятие конфиденциальности 5

1.2 Сведения, относящиеся к коммерческой тайне 8

1.3 Содержание государственной тайны 11

ГЛАВА 2. ПРИЕМ И УЧЕТ ВХОДЯЩИХ ДОКУМЕНТОВ, СОДЕРЖАЩИХ КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ 13

2.1 Прием входящих секретных документов 16

* 1. Секрет входящих секретных документов 18
	2. Работа с документами, содержащими конфиденциальные сведения 20

ЗАКЛЮЧЕНИЕ 23

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ 25

ВВЕДЕНИЕ

Данная курсовая работа посвящена очень важной и актуальной теме, а именно – приему и учету секретных документов. Важность и актуальность этой темы заключается в том, что защищаемые государством сведения в области его военной, разведывательной, контрразведывательной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации, играют очень важную роль в жизни человека, общества, государства.

Из-за стремительного развития Российской экономики и условий ужесточения конкуренции на рынке, организации подвергаются различным видам коммерческой слежки, в том числе – промышленному. В большинстве случаев предприятия используют бумажные носители. Как правило, они более практичней, удобней и долговечны в хранении. Но бумажные носители не имеют никакой степени безопасности, как, например, электронные, поэтому вся сохранность бумажных документов ложится на правильную организацию конфиденциального документооборота.

Деятельность многих организаций неразрывно связана с получением и использованием различного рода информации. В современных условиях информация представляет собой товар, имеющий определенную ценность. Часто наиболее ценной является информация, которую он использует для достижения целей организации и разглашение которой создает угрозы безопасности. Такую информацию называют конфиденциальной.

Конфиденциальная информация – это документированная (то есть зафиксированная на материальном носителе и с реквизитами, позволяющими ее идентифицировать) информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации. Часть этой коммерческой информации составляет особый блок и может быть отнесена к коммерческой тайне.

Цель работы - рассмотреть особенности работы с конфиденциальными документами, прием входящих секретных документов и их учет.

Поставленная цель достигается путём решения следующих задач:

1. Раскрыть понятие и содержание конфиденциальности;
2. Рассмотреть прием и учет входящих секретных документов;
3. Выявить сведения, которые относятся к коммерческой тайне;
4. Рассмотреть особенности подбора персонала для работы с документами, содержащими коммерческую тайну.

Объектом исследования настоящей работы является формирование и функционирование системы информационной безопасности в организации.

Предметом исследования является деятельность по обеспечению безопасности конфиденциальной информации в организации.

В процессе работы применялись исторический, логический методы, а также - специальные методы, используемые при исследовании правовых явлений, включая метод сравнительного правоведения.

Курсовая работа состоит из введения, заключения, списка используемой литературы и двух глав.

При написании данной курсовой работы были использованы следующие теоретические и эмпирические методы:

1. Теоретические методы (теоретический анализ учебной литературы, выделение и рассмотрение отдельных сторон, признаков, особенностей и свойств).

2. Эмпирические методы (наблюдение и изучение законодательных и нормативных материалов).

При написании курсовой работы были использованы разнообразные источники.

ГЛАВА 1. ПОНЯТИЕ О КОНФИДЕНЦИАЛЬНОСТИ, СВЕДЕНИЯ КОММЕРЧЕСКОЙ ТАЙНЫ И СОДЕРЖАНИЕ ГОСУДАРСТВЕННОЙ ТАЙНЫ

* 1. ПОНЯТИЯ КОНФЕЦИЦИАЛЬНОСТИ

Входящие секретные документы – это корреспонденция, поступающая

в орган внутренних дел.

Секретный документ - текстовые и графические материалы, выполненные любым способом, кино-, фото- и видео- позитивы и негативы, магнитные ленты звуко- и видеозаписи, перфокарты, перфоленты и другие материалы, которые содержат секретную информацию.

Конфиденциальная информация, включая коммерческую тайну, обычно содержится в виде любых документов-традиционных, бумажных или электронных. Эти источники информации могут подвергаться незаконным атакам и поэтому нуждаются в защите. Конфиденциальная информация на крупных предприятиях, имеющих нескольких собственников, является более сложным объектом защиты.

Цель режима секретности в системе делопроизводства – обеспечить информационную безопасность органов государственной власти. Можно сказать, более конкретно - обеспечить тайну тех сведений, которые могут быть использованы в ущерб интересам Российского государства.

Предприниматель в своей деятельности имеет дело с самой разнообразной информацией. Однако он не может всю информацию, которой обладает, сделать закрытой для внешних пользователей. С одной стороны, он должен предоставить максимум информации о своей деятельности потребителям, для того, чтобы они сделали выбор в его пользу. С другой стороны, предприниматель должен оградить названные группы лиц, а также своих конкурентов от информации, утечка или разглашение которой может представлять угрозу его экономической безопасности.

Получить информацию о деятельности фирмы можно двумя способами: законным и незаконным. Законный способ – это получение информации из средств массовой информации, рекламных проспектов фирмы, статей о фирме, с выставок, пресс-конференций. Эта информация специально готовится работниками фирмы для открытого пользования всеми заинтересованными лицами. Незаконный способ – это получение информации, не предназначенной для внешних пользователей, без согласия руководства фирмы, с нарушением действующего законодательства и приводящее к прямым экономическим потерям для фирмы, либо к упущенной выгоде.

В связи с этим, необходимо определить – какая, информация должна быть отнесена к коммерческой тайне и требует защиты. Важность информации определяется ее ценностью, которая, должна быть полезной своевременной, достоверной полной.

Строго конфиденциальная информация - это документы, утечка которых может вызвать тяжелые последствия для организации (предприятия, учреждения).

Конфиденциальная информация – ее разглашение наносит фирме ущерб, сопоставимый с текущими затратами фирмы, ущерб может быть преодолен в сравнительно короткие сроки.

Информация ограниченного доступа – ее утечка оказывает незначительное негативное воздействие на экономическое положение фирмы (должностные инструкции, структура управления).

Под безопасностью информационных ресурсов (информации) понимается защищенность информации во времени и пространстве от любых объективных и субъективных угроз (опасностей), возникающих в обычных экстремальных ситуаций.

Для более эффективной организации работы по защите коммерческой информации имеет смысл разработать и утвердить Положение о коммерческой тайне на предприятии. Этот документ строится на основе действующего законодательства, и отражает специфику данной организации (предприятия, учреждения) субъекта предпринимательства. Он включает перечень сведений, которые составляют коммерческую тайну, степень конфиденциальности информации, порядок доступа к информации и круг работников предприятия, допущенных к информации той или иной степени конфиденциальности.

Конфиденциальность – правила и условия сохранности передачи данных и информации. Различают конфиденциальность внешнюю – как условие неразглашения информации во внешнюю среду, и внутреннюю – то есть, среди персонала.

Таким образом, конфиденциальная информация это – информация, требующая защиты доступ к которой ограничивается в соответствии с действующим законодательством, а также настоящим Регламентом

1.2 СВЕДЕНИЯ, ОТНОСЯЩИЕСЯ К КОММЕРЧЕСКОЙ ТАЙНЕ

Чтобы понять, что же все таки означают секретные документы, нужно разобрать коммерческую тайну.

К коммерческой тайне могут быть отнесены самые разные сведения, связанные с производством и другими вопросами деятельности организации (предприятия, учреждения).

 Под коммерческой тайной также могут подразумевать саму информацию, которая составляет коммерческую тайну, то есть, научно-техническую, технологическую, производственную, финансово-экономическую, военную или иную информацию, в том числе составляющую секреты производства, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности её третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введён режим коммерческой тайны.

Сведения, относящиеся к коммерческой тайны:

1. Коммерческие данные конфиденциального характера;
2. Ценообразование и стоимостные показатели закупаемую и реализуемую продукцию;
3. Планы коммерческой и хозяйственной деятельности;
4. Обязательства, контрактные соглашения;
5. Информация, касающаяся коммерческих нововведений;
6. Информационный процесс и коммерческие сведения, накопленные электронно.

Обладатель информации принимает меры к охране ее конфиденциальности. Информация может быть разделена на три категории.

Первая – несекретная (или открытая), которая предназначена для использования как внутри фирмы, так и вне ее.

Вторая – для служебного пользования, которая предназначена только для использования внутри фирмы. Она подразделяется, в свою очередь, на две категории:

1. Доступную для всех сотрудников фирмы.
2. Доступную для определенных сотрудников.

Третья – секретная информация (или информация ограниченного доступа), которая предназначена для использования только специально уполномоченными сотрудниками фирмы и не предназначена для передачи иным сотрудникам в полном объеме или по частям.

Критерии, при которых информация может быть отнесена к конфиденциальной, перечислены в ст. 13 части 1 ГК РФ. К ним отнесены:

1. Коммерческая ценность информации в силу ее неизвестности третьим лицам;
2. Отсутствие свободного доступа к этой информации на законном основании;
3. Обеспечение мер безопасности для конфиденциальной информации.

В организационном плане работу по определению сведений,  которые составляют коммерческую тайну, можно разделить на следующие три этапа.

На первом этапе будет  необходимо издать приказ, устанавливающий порядок определения сведений, которые составляют коммерческую тайну.

В этом приказе следует указать следующую информацию:

* Состав постоянно действующей комиссии по коммерческой тайне;
* Категории персонала, которому предоставляется право предварительной классификации информации как коммерческая тайна порядок документирования работы по определению сведений, составляющих коммерческую тайну;
* Сроки подготовки перечня сведений, которые составляют коммерческую тайну и его представление для утверждения руководством.

На втором этапе постоянно действующей комиссии должна проанализировать возможный ущерб от утечки выделенных на первом этапе сведений.

Третий этап сводится к формированию перечня сведений, которые составляют коммерческую тайну предприятия, и вводу перечня в действие.

Работник обязан строго хранить в тайне сведения, отнесенные к коммерческой тайне предприятия, ставшие ему известными по службе или иным путем. Разглашение коммерческой тайны предприятия, передача третьим лицам, публикация без согласия предприятия, а также использование для занятия любой деятельностью, которая в качестве конкурентного действия может нанести ущерб предприятию, влечет уголовную, административную, гражданско-правовую или иную ответственность в соответствии с законодательством.

* 1. СОДЕРЖАНИЕ ГОСУДАРСТВЕННОЙ ТАЙНЫ

Государственная тайна - это информация, охраняемая государством в сфере его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которой может нанести ущерб Российской Федерации.

Государственную тайну составляют: сведения в военной области, сведения в области экономики, сведения в области внешней политики, сведения в области разведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму.

Отнесение сведений к государственной тайне и засекречивание этих сведений осуществляется на основе принципов: законности, обоснованности, своевременности отнесения сведений к государственной тайне.

Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения таких сведений. При засекречивании сведений им устанавливается три степени секретности и соответствующие этим степеням грифы секретности для носителей таких сведений:

1. Особой важности;
2. Совершенно секретно;
3. Секретно.

Основанием для рассекречивания сведений являются: взятие Российской Федерации на себя международных обязательств по открытому обмену сведениями, составляющими государственную тайну; и изменение объективных обстоятельств, вследствие которого дальнейшая защита таких сведений является нецелесообразной.

Срок засекречивания сведений, составляющих государственную тайну, не должен превышать 30 лет. В исключительных случаях этот срок может быть продлен межведомственной комиссией по защите государственной тайны.

Система защиты государственной тайны – это совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну и их носителей, а также мероприятия, проводимые в этих целях.

К органам защиты государственной тайны относят: межведомственную комиссию по защите государственной тайны, федеральную службу безопасности, министерство обороны, федеральную службу внешней разведки.

Контроль за обеспечением защиты государственной тайны осуществляют Президент Российской Федерации и Правительство Российской Федерации. Надзор за соблюдением законодательства при обеспечении защиты государственной тайны и законностью принимаемых при этом решений осуществляет Генеральный прокурор РФ и подчиненные ему прокуроры.

Основаниями для отказа должностному лицу или гражданину в допуске к государственной тайне могут являться:

* Признание его судом недееспособным, ограниченно дееспособным;
* Признание его рецидивистом;
* Нахождение его под судом или следствием за государственные или иные тяжкие преступления, наличие у него неснятой судимости;
* Наличие у него медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну;
* Постоянное проживание его самого и (или) его близких родственников за границей или оформление указанными лицами документов для выезда на постоянное место жительства в другие страны;
* Выявление в результате проверочных мероприятий действий оформляемого лица, создающих угрозу безопасности РФ;
* Уклонение его от проверочных мероприятий и (или) сообщение им заведомо ложных анкетных данных.

Допуск лица к государственной тайне может быть прекращен по решению руководителя органа власти, предприятия, организации в случаях:

1. Расторжения трудового договора в связи с проведением организационных или штатных мероприятий;

 2. Однократного нарушения им взятых на себя обязательств, связанных с защитой государственной тайны;

3. Возникновения обстоятельств, предусмотренных законом (признание недееспособным, судимость и т.п.).

Прекращение допуска к государственной тайне не освобождает гражданина от взятых им обязательств по неразглашению сведений, составляющих государственную тайну.

ГЛАВА 2. ПРИЕМ И УЧЕТ ВХОДЯЩИХ ДОКУМЕНТОВ, СОДЕРЖАЩИХ КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ

2.1 ПРИЕМ ВХОДЯЩИХ СЕКРЕТНЫХ ДОКУМЕНТОВ

Входящий документ— это документ, поступивший на предприятие, в организацию, учреждение. Входящие (поступающие) документы могут быть доставлены по почте, курьером, по факсу, электронной почтой. Большую часть входящих документов составляет переписка.

Прием и регистрацию документов, содержащих конфиденциальную информацию, осуществляют государственные гражданские служащие отдела-канцелярии (правительственная корреспонденция) и отдела общей корреспонденции Управления делами в соответствии с должностными обязанностями, возложенными на них должностными регламентами.

Работники предприятия, допущенные к конфиденциальным сведениям и документам, прежде чем получить доступ к ним, должны пройти инструктаж и ознакомиться с памяткой о сохранении коммерческой тайны предприятия. Памятка составляется службой безопасности с учётом специфики конкретного предприятия, подписывается заместителем директора и утверждается директором предприятия.

Ведение делопроизводства, обеспечивающего учёт и сохранность документов, содержащих коммерческую тайну, предусматривает выполнение ряда рекомендаций.

При получении пакетов государственный гражданский служащий должен:

1. Проверить на пакете наличие пометки "Для служебного пользования", "ДСП" и т.п.;
2. Убедиться, что содержимое пакета не просматривается;
3. Проверить целостность упаковки документа;
4. Проверить соответствие вложенных в пакет документов описи или ссылке на приложение к сопроводительному письму.

При поступлении пакета с поврежденной упаковкой составляется акт в трех экземплярах к настоящей Инструкции, который подписывается начальником отдела-канцелярии (правительственная корреспонденция) либо начальником отдела общей корреспонденции Управления делами и лицом, доставившим пакет (при поступлении пакета по почте - государственным гражданским служащим, принимавшим почту).

При обнаружении признаков несанкционированного вскрытия конверта об этом сразу докладывается заместителю руководителя ФАС России, координирующему и контролирующему деятельность Управления делами, который принимает решение о приеме пакета. При этом составляется акт в двух экземплярах, один экземпляр которого направляется отправителю, а второй экземпляр подшивается в дело согласно номенклатуре дел Управления делами.

При передаче документов, содержащих коммерческую тайну, в органы государственной власти и органы местного самоуправления гриф «Коммерческая тайна» или «Конфиденциально» проставляется в обязательном порядке.

В тексте документа также может быть оговорена конфиденциальность сведений, права предприятия на них, порядок их использования и т.п. Например, если коммерческая тайна является результатом совместной деятельности с другим предприятием, то необходимость её сохранения должна быть отражена в договоре.

Входящие документы с грифом "Коммерческая тайна", содержащие персональные данные физических лиц - собственников основных производственных средств, нематериальных активов, владельцев ценных бумаг, после регистрации передаются для последующей работы с ними в Отдел защиты информации.

Ответственный государственный гражданский служащий Управления делами вносит реквизиты документа в журнал учета входящей корреспонденции "ДСП" к настоящей Инструкции и передает документ под роспись в журнале государственному гражданскому служащему управления.

Печатание документов с грифом «Коммерческая тайна» производится централизованно, в специально отведённом помещении, исключающем доступ посторонних лиц.

Все документы, содержащие конфиденциальную информацию, должны регистрироваться отдельно от остальной документации в Журнале регистрации документов с грифом «Коммерческая тайна». При значительном объёме документов могут быть заведены журналы отдельно для входящих, исходящих и внутренних документов предприятия, содержащих гриф «Коммерческая тайна».

Хранятся такие дела в сейфе, который опечатывается должностным лицом, ответственным за сохранность документов с грифом «Коммерческая тайна». Другие работники предприятия не должны иметь доступа к этому сейфу.

На поступивших в организацию с сопроводительным письмом приложениях пишут от руки или проставляют с помощью штампа отметку «к вх. №\_от\_», в которой указывают входящий номер и дату регистрации сопроводительного документа. Данную отметку проставляют в правом нижнем углу первого листа прилагаемого бумажного документа, на обложке и титульном листе документа выделенного хранения. В случае поступления в организацию внешних электронных носителей конфиденциальной информации отметку наносят специальным маркером на внешнюю поверхность дисков.

Поступившие в организацию с сопроводительным письмом внешние электронные носители конфиденциальной информации учитывают в журнале учета внешних электронных носителей конфиденциальной информации. Если в организацию поступили бумажные документы, не подлежащие подшивке в дела, их ставят на инвентарный учет с присвоением соответствующего инвентарного номера по журналу учета конфиденциальных документов выделе иного хранения.

В относительно большой организации со сложной структурой, где делопроизводство ведется не только в подразделении, отвечающем за прием и учет корреспонденции, но и в других структурных подразделениях, конфиденциальное делопроизводство будет расширенным. Поток входящей корреспонденции при этом разделится на множество ручейков для каждого из этих подразделений.

2.2 УЧЕТ СЕРЕТНХ ДОКУМЕНТОВ

Учет секретных документов - регистрация и контроль за их сохранностью. Существует 2 формы учета секретных документов: журнальная и карточная. При журнальной системе информация о секретных документов хранится в специальных журналах. При карточной - на специальных карточках, отельных 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, спец. блокноты, отдельные листы бумаги.

Базовый порядок работы с входящей, исходящей и внутренней конфиденциальной корреспонденцией в организации устанавливается в соответствии с требованиями локальных нормативных актов, регламентирующих процессы делопроизводства для открытых документов. Вместе с тем работа с конфиденциальной корреспонденцией имеет некоторые особенности.

На поступивших в организацию с сопроводительным письмом приложениях пишут от руки или проставляют с помощью штампа отметку в которой указывают:

Входящий номер и дату регистрации сопроводительного документа. Данную отметку проставляют в правом нижнем углу первого листа прилагаемого бумажного документа, на обложке и титульном листе документа выделенного хранения. В случае поступления в организацию внешних электронных носителей конфиденциальной информации отметку наносят специальным маркером на внешнюю поверхность дисков.

Поступившие в организацию с сопроводительным письмом внешние электронные носители конфиденциальной информации учитывают в журнале учета внешних электронных носителей конфиденциальной информации. Если в организацию поступили бумажные документы, не подлежащие подшивке в дела, их ставят на инвентарный учет с присвоением соответствующего инвентарного номера по журналу учета конфиденциальных документов выделе иного хранения.

В относительно большой организации со сложной структурой, где делопроизводство ведется не только в подразделении, отвечающем за прием и учет корреспонденции, но и в других структурных подразделениях, конфиденциальное делопроизводство будет расширенным. Поток входящей корреспонденции при этом разделится на множество ручейков для каждого из этих подразделений.

2.3 РАБОТА С ДОКУМЕНТАМИ, СОДЕРЖАЩИМИ КОНФИДЕНЦИАЛЬНЫЕ СВЕДЕНИЯ

На предприятии должен быть принят строгий порядок размножения документов с грифом «Коммерческая тайна». Они должны копироваться с разрешения руководства предприятия в специально выделенном помещении. Все копии конфиденциальных документов берутся на учёт в специальном журнале или в Журнале регистраций документов с грифом «Коммерческая тайна». Количество экземпляров документов с грифом «Коммерческая тайна» должно быть ограничено, причём каждый экземпляр готовится для заранее определённого адресата или исполнителя. Размножение документов следует производить в присутствии должностного лица, ответственного за документ. Все бракованные копии документа им забираются и подлежат немедленному уничтожению.

При работе с конфиденциальными документами необходимо ввести ряд следующих ограничений для работников предприятия:

- запрещается делать выписки из документов, имеющих гриф ограничения доступа, без письменного разрешения руководителя;

- запрещается знакомиться с документами, делами, информацией, содержащейся в памяти компьютера, других работников предприятия;

Ограниченного доступа, в открытых докладах, сообщениях, переписке, рекламных изданиях;

- запрещается предоставлять свой компьютер для работы другим сотрудникам предприятия и работать на их ПК;

- запрещается бесконтрольно оставлять конфиденциальные документы на рабочем столе и работающий компьютер с конфиденциальной информацией.

Все дела с грифом «Коммерческая тайна» и журналы их учёта вносятся в номенклатуру дел предприятия. В том случае, если заголовки дел несут элементы коммерческой тайны, могут применяться условные заголовки дел или составляться отдельная номенклатура только на эти дела.

По окончании года специально созданная комиссия предприятия выполняет следующие работы:

- проверяет наличие всех документов с грифом «Коммерческая тайна»;

- отбирает документы с грифом «Коммерческая тайна» для архивного хранения;

- отбирает документы с грифом «Коммерческая тайна» для уничтожения.

Проверка наличия документов с грифом «Коммерческая тайна» по решению руководства предприятия может производиться с другой периодичностью, например, по окончании полугодия.

В случае установления факта утраты документов с грифом «Коммерческая тайна» немедленно ставится в известность руководитель предприятия, служба безопасности и принимаются все меры к розыску документа. Руководителем предприятия в связи с фактом утраты назначается комиссия для служебного расследования.

На утерянные документы после того, как розыск их не принёс положительных результатов, составляется акт. В «Журнал регистрации документов с грифом «Коммерческая тайна» вносятся соответствующие отметки об утрате.

При увольнении сотрудника, ответственного за документы с грифом «Коммерческая тайна», производится проверка числящихся за ним документов и их передача вновь назначенному лицу. Акт приёма – передачи этих документов утверждается руководителем предприятия или его заместителем.

При прекращении трудовых отношений с предприятием, на котором сотрудник был допущен к коммерческой тайне, обязательства о неразглашении конфиденциальных сведений действуют в течение двух лет, если иной срок не установлен трудовым договором.

При передаче дел в архив на документы с грифом «Коммерческая тайна» составляется отдельная опись.

Архивное хранение таких документов производится в опечатанных коробках, в помещениях, исключающих несанкционированный доступ.

На документы с грифом «Коммерческая тайна», отобранные для уничтожения, составляется акт, утверждаемый руководителем предприятия. Уничтожаются документы в присутствии комиссии с помощью специальной машины или иным способом, исключающим возможность восстановления имеющейся в них информации.

Руководитель предприятия по согласованию со службой безопасности может устанавливать дополнительные меры защиты документов по собственному усмотрению, например, ограничение круга должностных лиц, имеющих доступ к конфиденциальным сведениям, использование технических средств для обеспечения сохранности документов.

ЗАКЛЮЧЕНИЕ

Для обеспечения сохранности и неразглашения конфиденциальных сведений предприятия необходимо выполнение самых простых требований безопасности, профессиональное обучение персонала требованиям работы с конфиденциальными документами, материальное стимулирование руководством организации сотрудников, имеющих доступ к документам с грифом «Коммерческая тайна», правильная организация секретного делопроизводства и документооборота на предприятии.

 Строгое привлечение к ответственности сотрудников предприятия за нарушение норм и инструкций по секретному делопроизводству. Сведения к минимуму несанкционированного доступа к конфиденциальной документации можно достичь путём увеличения различных административных, технологических и других барьеров. Это делается для того, чтобы организация хищения конфиденциальных сведений предприятия влекло за собой значительные финансовые, материальные и иные траты, которые неоправдывали бы риск и затраченные на это усилия. На мой взгляд, данное условие сильно бы сократило несанкционированные утечки конфиденциальных сведений организации, что, конечно, и дорогостояще, но в наше время бы сильно помогло предприятиям конкурировать на рынке.

В настоящее время органы внутренних дел представляют собой систему, в которой скапливается огромное количество социально значимой информации, значительная часть которой требует действенной системы защиты, однако приспособление ранее существовавшей в ОВД схемы обеспечения сохранности государственной тайны к современным условиям протекает крайне медленно.

Таким образом, можно сделать выводы, что в современном обществе появилась необходимость в открытости и доступности, в частности своевременное и свободное получение сведений о деятельности законодательной, исполнительной и судебной власти. Причем речь идет о данных, представляющих личный, государственный и общественный интересы. Также начала проявляться еще одна крайность - стремление к максимальной информационной открытости, облегченно-пренебрежительное отношение к вопросам конфиденциальности и обеспечению режима секретности в работе с документами.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. <https://studref.com/470027/dokumentovedenie/uchet_konfidentsialnyh_dokumentov>, 2017
2. <https://sudact.ru/law/prikaz-miniusta-rossii-ot-19052008-n-110/prilozhenie/iii/uchet-sekretnykh-i-rassekrechennykh-arkhivnykh/>, 2016
3. <https://referatbank.ru/market/referat/i/414891/kursovaya-rezhim-sekretnosti-dokumentov.html>, 2018
4. <https://referat.bookap.info/work/176860/Poryadok-raboty-s-sekretnymi>, 2018
5. <https://studopedia.ru/6_99898_poryadok-raboti-s-sekretnimi-dokumentami.html>, 2019
6. <https://www.yaneuch.ru/cat_87/rabota-s-sekretnymi-dokumentami/10527.609294.page1.html>, 2016
7. <http://www.tsutmb.ru/nauka/internet-konferencii/2017/inform-i-documen-obespechenie-6/3/tsvetkova.pdf>, 2016
8. <http://55referatov.ru/doc/referaty_na_voennye_temy/voennoe_delo/4628-osnovy_rezhima_sekretnosti.php?PAGEN_2=5>, 2019
9. <https://www.std72.ru/dir/deloproizvodstvo/dokumentacionnoe_obespechenie_upravlenija_uchebnoe_posobie/12_rabota_s_konfidencialnymi_dokumentami/239-1-0-4358>, 2017
10. <https://fb.ru/article/301461/sekretnoe-deloproizvodstvo-organizatsiya-i-pravila-vedeniya>, 2017
11. <https://sudact.ru/law/prikaz-miniusta-rossii-ot-19052008-n-110/prilozhenie/iii/uchet-sekretnykh-i-rassekrechennykh-arkhivnykh/>, 2016