Организация работы с документами, содержащими коммерческую тайну

Практически в любой организации рано или поздно встает вопрос защиты информации и организации работы с информацией, отнесенной к коммерческой тайне.

Далее мы будем рассматривать организацию работы с документами, содержащими коммерческую тайну и закрепленными на бумажных носителях. (Средства технической защиты и требования к служебным помещениям в данной статье не рассматриваются.)

С.Л. Орлова,
эксперт в сфере ДОУ, член Гильдии управляющих документацией

Под информацией, составляющей коммерческую тайну, в соответствии с Федеральным законом от 29.07.2004 № 98-ФЗ **«О коммерческой тайне»** (далее – ФЗ «О коммерческой тайне») понимается научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства – ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны.

В статье 5 ФЗ «О коммерческой тайне» приведен перечень сведений, которые не могут составлять коммерческую тайну.

С чего начать организацию работы с конфиденциальной информацией?

Конечно же, с определения сведений, относимых к коммерческой тайне. Для этого руководителю организации необходимо создать **экспертную комиссию по отнесению сведений к категории «коммерческая тайна».**

Комиссия при выделении из общего информационного массива конфиденциальных сведений должна руководствоваться следующими принципами:

- информация должна быть коммерчески выгодна для организации или для конкурентов;
- информация не должна быть общедоступной на законных основаниях;
- информация должна быть зафиксирована на материальном носителе, принадлежащем организации, и находиться в ведении этой организации;
- информация не должна касаться запрещенной или незакрепленной в уставе организации деятельности, носить незаконный характер, содержать сведения и инструкции к действиям, которые могут нанести вред окружающей среде, здоровью граждан и т. п.

Результатом проделанной Комиссией работы должен служить выпущенный **Перечень информации, отнесенной к коммерческой тайне.** Данный документ может быть введен как отдельно, приказом по организации, так и в качестве приложения к Положению о конфиденциальной информации. Никаких специальных требований по оформлению данного документа нет.

После выявления сведений, содержащих коммерческую тайну, следует приступить к разработке пакета документов, определяющих порядок работы с документами, содержащими коммерческую тайну.

Как правило, вполне достаточно двух документов: **Положения о конфиденциальной информации** и **Инструкции по работе с документами, составляющими коммерческую тайну.**

Мы рекомендуем при разработке **Положения о конфиденциальной информации** включить в него следующие разделы:

Раздел	Содержание
1	2
Общие положения	В данном разделе нужно кратко описать предназначение данного документа, раскрыть основные понятия (конфиденциальная информация), дать ссылку на федеральные законы.

Словарь

Конфиденциальный (от лат. confidentiale – доверие) **документ** – доверительный, секретный документ.

Коммерческая тайна – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

1	2
Правила категорирования конфиденциальной информации	Российское законодательство предоставляет коммерческим организациям возможность использовать только один гриф «Коммерческая тайна». Коммерческие организации не могут использовать даже гриф «ДСП» (для служебного пользования). Но такие жесткие рамки не всегда удобны в работе. Поэтому можно ввести категорирование информации, т. е. когда документам, выпускаемым под грифом «Коммерческая тайна», разрешается присваивать некие дополнительные категории, позволяющие внутри организации разграничивать, например, степень допуска сотрудников к данным документам, порядок обработки документов той или иной категории
Защита информации	В данном разделе перечисляются меры, принимаемые в организации для защиты информации: определение перечня информации, составляющей коммерческую тайну; ограничение доступа; учет лиц, получивших доступ к данной информации; регулирование отношений по использованию данной информации работниками на основании трудовых договоров; нанесение данной информации на материальные носители; нанесение грифа; нанесение категорий (если есть); порядок доступа к данной информации, ее хранения и уничтожения
Допуск к конфиденциальной информации, составляющей коммерческую тайну	Оговариваются категории сотрудников, имеющих право доступа к информации, содержащей коммерческую тайну. Далее оговаривается порядок действий, который необходимо выполнить сотрудникам для получения допуска к информации, содержащей коммерческую тайну, а также перечисляются условия, при наступлении которых доступ сотрудников к данной информации может быть прекращен
Передача и предоставление конфиденциальной информации	В данном разделе оговаривается порядок предоставления информации по запросам государственных организаций: запрос должен быть мотивирован – т. е. указана цель и правовое обоснование затребованной информации. Запрос должен быть заверен подписью должностного лица, уполномоченного запрашивать конфиденциальную информацию, объявлен срок предоставления этой информации, если иное не предусмотрено законом. Также определяется перечень подразделений, осуществляющих взаимодействие с органами государственной власти и управления в рамках их функционала, и порядок их взаимодействия с этими органами
Защита конфиденциальной информации в процессе служебной деятельности	Оговаривается обязательность защиты сведений, составляющих коммерческую тайну, и ответственность сотрудников, получивших доступ к данной информации. Также оговариваются порядок обращения с данными документами, условия их хранения, передачи, перевозки, порядок действия при наступлении форс-мажорных обстоятельств
Охрана конфиденциальной информации в процессе неслужебных контактов	В данном разделе оговаривается порядок действий сотрудников при попытке посторонних лиц получить информацию, составляющую коммерческую тайну, или при обнаружении фактов утечки или утраты документов, содержащих конфиденциальную информацию
Ответственность за нарушение режима конфиденциальности	В данном разделе определяется – что понимается под разглашением конфиденциальной информации, какая ответственность наступает в случае разглашения конфиденциальной информации или в случае утраты документов, содержащих конфиденциальную информацию

При разработке **Инструкции по работе с документами, составляющими коммерческую тайну,** необходимо помимо основных пунктов Инструкции по делопроизводству включить следующие положения:

- **порядок выноса-вноса конфиденциальных документов на охраняемой территории;**
- **порядок работы с конфиденциальными документами вне служебных помещений;**
- **порядок изготовления и использования бланков организации, печатей и штампов;**

- **порядок использования бланков строгой отчетности (бланков организации, подготавливаемых за подписью первых лиц организации);**
- **порядок передачи конфиденциальных документов в случае ухода сотрудников в отпуск, отъезда в командировку или увольнения с работы;**
- **порядок подготовки конфиденциальных документов, их согласование, в том числе с юристами, финансистами, корректорами, а также порядок подписи конфиденциальных документов;**
- **порядок пересылки конфиденциальных документов вне контролируемых помещений.**

После утверждения **Положения о конфиденциальной информации** каждый сотрудник организации должен быть ознакомлен с данным документом под расписку, а также подписать **Обязательство о неразглашении** коммерческой тайны, ставшей известной в период работы в данной организации (см. приложение).

Все вновь пришедшие в организацию работники должны подписывать такой документ при приеме на работу после ознакомления с Положением о конфиденциальной информации.

Организация конфиденциального делопроизводства

При любой форме конфиденциального делопроизводства в организации основные функции документирования должны оставаться централизованными:

получение, отправка, регистрация документов, тиражирование (копирование), протоколирование совещаний, набор текста (машинопись, стенографирование).

Поэтому типовая структура службы ДОУ организации с количеством сотрудников более 1000 чел. и значительным объемом документов, содержащих коммерческую тайну, должна непременно включать:

группу по подготовке документов (машбюро, стенографическое бюро, копировальное бюро), канцелярию (экспедицию, регистратуру), группу контроля исполнения решений, группу контроля за соблюдением мер и требований по ведению конфиденциального делопроизводства, архив документов на бумажных и других типах носителей информации, а также подразделения технической защиты информации.

В учреждениях с меньшим объемом документов, содержащих коммерческую тайну, остаются те же функции, но они требуют участия гораздо меньшего количества сотрудников.

Это могут быть сотрудники секретариата (2–5 человек), возможно, один секретарь, если в организации работает до 50 чел.

Если в небольшой организации в секретариате работает 5 чел., целесообразно закрепить участок по ведению конфиденциального делопроизводства за двумя сотрудниками – здесь нужно сразу учитывать проблему взаимозаменяемости.

Важно знать!

Ведение конфиденциального делопроизводства рекомендуется закреплять за наиболее опытными сотрудниками.

Конфиденциальное делопроизводство базируется на тех же принципах, что и простое, но отличается большим количеством видов работ, которые начинаются с момента создания документа.

Подготовка и печать документов

Подготовка и печать документов, содержащих конфиденциальную информацию, производятся: с черновика, написанного сотрудником собственноручно или стенографисткой под диктовку; сотрудником самостоятельно, без черновика, в специально оборудованном помещении, на компьютерах, прошедших специальную проверку.

Все черновики подлежат учету в карточке (журнале) машинописных работ и после получения сотрудником отпечатанного экземпляра документа подлежат немедленному уничтожению, о чем производится запись в учетной форме и ставится подпись сотрудника – владельца черновика и сотрудника службы ДОУ, уполномоченного по ведению конфиденциального делопроизводства, уничтожившего черновик.

Помещения, в которых происходит диктовка и набор документов, должны быть закрыты от общего доступа, стены и потолки обшиты средствами звукоизоляции.

Черновики конфиденциальных документов должны подготавливаться в специальных блокнотах, имеющих в верхнем правом углу каждого листа гриф **коммерческая тайна** (по заполнении). Все листы в спецблокнотах должны быть пронумерованы. После использования всего блокнота сотрудник, которому был выдан блокнот, обязан сдать в службу ДОУ сотруднику, уполномоченному по ведению конфиденциального делопроизводства, корешок спецблокнота с подложкой, на которой при выдаче был проставлен учетный номер.

На заметку!

На небольшом количестве предприятий уже есть внедреннные системы конфиденциального делопроизводства. При электронной форме организации делопроизводства учет и движение документов контролировать гораздо удобнее.

Такой учет спецблокнотов необходим, так как минимизирует риски попадания неучтенных черновиков в обычные корзины для бумаг, что может привести к серьезной утечке информации. По той же технологии учитываются и сдаются на уничтожение спецтетради стенографисток.

Все блокноты учитываются в специальных журналах.

Если черновик составляется на машинном носителе (диск, дискета и пр.), необходимо организовать учет таких носителей следующим образом:

- Компьютер сотрудника должен пройти аттестацию в службе безопасности предприятия.
- Носители для записи конфиденциальной информации должны быть пронумерованы и выдаваться сотрудником отдела средств технической защиты другим сотрудникам под роспись в журнале учета.
- При нанесении информации, переносе ее на другой носитель, отправке, возврате, стирании – при каждом действии сотрудником данного отдела производится запись в журнале.
- По истечении срока годности магнитные носители подлежат сдаче в отдел средств технической защиты для утилизации.

Регистрация документов

После утверждения документы должны быть зарегистрированы путем присвоения им порядковых номеров в журнале регистрации. Если документ составлен совместно несколькими организациями, то его регистрационный номер будет состоять из нескольких номеров – по количеству организаций.

В крупных организациях при больших объемах документов преобладает карточная система учета конфиденциальных документов.

Тиражирование и рассылка

После регистрации уполномоченный сотрудник службы ДОУ снимает с документа необходимое количество копий согласно предоставленному списку рассылки. На каждом экземпляре документа под грифом проставляется номер экземпляра и получатель.

После тиражирования и учета (карточная форма учета более эффективна) документы отправляются адресатам:

внутри организации при централизованной форме конфиденциального делопроизводства документы передаются через уполномоченных по ведению конфиденциального делопроизводства под расписку либо лично сотруднику-исполнителю (также под расписку).

Организация контроля исполнения

Организация контроля исполнения документов, содержащих коммерческую тайну, выстраивается аналогично контролю в делопроизводстве: службы ДОУ отвечают за сроковый контроль, контроль по существу вопроса возлагается на наиболее опытного сотрудника организации, знающего все действующие бизнес-процессы в организации.

На заметку!

При наличии электронной системы конфиденциального делопроизводства вся информация отправляется на личные адреса исполнителей.

Подготовка документов к архивному хранению

Подготовка документов к архивному хранению производится на основании утвержденной номенклатуры дел – перечня заголовков дел с указанием их сроков хранения. При определении сроков хранения на документы, составляющие коммерческую тайну, используют номенклатуру дел общего делопроизводства.

Исполненные документы передаются в службу ДОУ и подшиваются в дела.

При централизованной форме ведения конфиденциального делопроизводства исполнитель в левом нижнем углу основного документа проставляет отметку «В дело» с комментарием, чем решен вопрос. Затем указывает свою должность, проставляет подпись, расшифровку подписи и дату. Уполномоченный сотрудник службы ДОУ проверяет сданные документы, о сдаче документов делается соответствующая запись в карточке (журнале, в СЭД), проставляет свою подпись и дату. После формирования документов в дела уполномоченный сотрудник службы ДОУ проставляет в карточке (журнале, СЭД) номер дела.

При формировании в дела документов делу под грифом «Коммерческая тайна» присваивается высшая категория (если категорирование документов, содержащих коммерческую тайну, закреплено в Положении о конфиденциальной информации). Дела могут формироваться по видам документов, по предметно-вопросному признаку, по алфавитному, по контрагентам, по географическому признаку и т. п. Формирование дел производится на основании «Инструкции по работе с документами, содержащими коммерческую тайну». Составляется внутренняя опись дела с указанием всех разделов и документов (номер, дата, листаж, краткое содержание документов, количество листов), подшитых в нем. Дела прошиваются в четыре прокола, пломбируются, опечатываются таким образом, чтобы были захвачены оба конца нити, на обложке делается заверительная надпись: в деле _____ подшито и пронумеровано _____ листов. Ставится должность, подпись, расшифровка подписи сотрудника, подготовившего дело, дата.

После окончания календарного года дела передаются на архивное хранение в архив.

Мнение эксперта

Г.В. Подкорытова,
начальник отдела делопроизводства ЗАО «ФИНЭКС Качество», член Гильдии управляющих документацией

Вопросы деятельности организации, связанные с защитой конфиденциальной информации, бесспорно, очень актуальны.

Формы организации конфиденциального делопроизводства (КД), как правило, определяются численным составом организации, направлением вида деятельности, формой собственности и могут быть следующими:

- Организация и ведение работы с КД закрепляются за определенным работником службы (отдела), отвечающей за организацию работы с документами, – это может быть ДОУ.
- В составе службы (отдела) ДОУ создается подразделение (группа) конфиденциального делопроизводства.
- В состав штатной структуры организации вводится самостоятельное подразделение КД. Оно может подчиняться непосредственно руководителю организации или его заместителю, курирующему вопросы КД.
- Подразделение конфиденциального делопроизводства может входить в состав других подразделений, как правило, осуществляющих защиту конфиденциальной информации: службу безопасности, службу защиты информации и др.

Структура и статус подразделения КД определяются объемом конфиденциального делопроизводства и штатной расстановкой предприятия.

Численный состав сотрудников подразделения конфиденциального делопроизводства может быть определен с учетом норм времени на выполнение необходимого объема работ.

Отдельно хотелось бы сказать о преимуществах работы с КД в электронном виде. Здесь речь идет, несомненно, о работе с КД в системе электронного документооборота.

В недалеком прошлом я, начальник отдела делопроизводства крупного машиностроительного завода, не могла не отметить очевидные преимущества и эффективность внедрения СЭД «DIRECTUM» в работе с документами, в т. ч. конфиденциальными.

Одной из важнейших функциональных задач, поставленной при внедрении СЭД, являлась защита информации от несанкционированного доступа. Конфиденциальность документов, хранящихся в СЭД, обеспечивалась следующими возможностями:

- Контроль и настройка прав доступа на любой объект системы (полный доступ, изменение, просмотр, полное отсутствие доступа), обеспечивающие защиту от несанкционированного доступа.
- Шифрование, позволяющее защитить текст электронного документа от пользователя. Конфиденциальные электронные документы и задачи могут быть зашифрованы непосредственно в системе любым совместимым криптопровайдером (в т. ч. сертифицированным ФСБ), что гарантирует защиту даже от лиц, имеющих неограниченный доступ к данным (администраторов системы).
- Протоколирование всех действий пользователей, позволяющее быстро установить историю работы с документом и проконтролировать такие действия над документом, как просмотр, изменение, экспорт копии документа и пр., в т. ч. в случае нарушения режима безопасности. Обеспечивается высокая защита от несанкционированного доступа к хранилищам документов всех типов.

В заключение хочется отметить – далеко не на всех коммерческих предприятиях принимаются должные меры по сохранности информации ограниченного доступа. Сегодня, к сожалению, мы должны признать, что ресурсы утечки информации все-таки имеют место. А это в свою очередь приводит к утрате интеллектуальной собственности предприятия, упущенной выгоде и иным негативным явлениям в ходе выполнения наших общих целей и задач.

Изъятие документов из дел разрешается в случае необходимости руководителем подразделения, отвечающим за архивное хранение документов на основе заявки, согласованной в установленном порядке. В этом случае дело расшивается, внутрь вставляется лист-заместитель. По возвращении документа дело вновь прошивается, делается заверительная надпись. Если документ изъят безвозвратно, в дело подшивается его заверенная копия, в описи делается соответствующая отметка. Такое на практике случается редко.

Обычно в архиве дела запрашиваются целиком. Дела для ознакомления выдаются сотрудникам в специально оборудованном архивном помещении – читальном зале. На дело заводится карточка учета выдачи дела. Все дела выдаются под расписку с указанием даты выдачи и даты возврата. В случае необходимости с документа, подшитого в дело, снимаются копии, которые регистрируются в установленном порядке и передаются сотруднику предприятия под расписку. Дело же возвращается в архив.

Выделение дел к уничтожению

По истечении сроков хранения дел на них составляется акт о выделении к уничтожению. Если заголовки дел не содержат конфиденциальной информации (обезличены), гриф на акт не присваивается. При наличии грифа акт регистрируется как изданный документ.

Перед уничтожением включенных в акт дел проверяется соответствие данных акта записям в протоколе ЭК, журналах (карточках) регистрации, о соответствии данных делается запись в акте.

Уничтожение дел должно производиться путем сжигания или в шредерах с высокой степенью измельчения материала. После уничтожения производятся отметки об уничтожении дел и учетных журналов (картотек) в номенклатуре дел.

Проверка наличия документов, содержащих коммерческую тайну

Проверки наличия документов, содержащих коммерческую тайну, могут быть регламентированными (квартальными, годовыми) и нерегламентированными (при смене руководителя первого отдела, при выявленных нарушениях режима работы с документами, при ликвидации предприятия).

Цель проводимых проверок – контроль за сохранностью информации и за соблюдением режима работы.

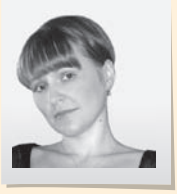
Во время проверок помимо наличия документов и носителей проверяется также правильность регистрации данных материалов.

Проверки должны проводиться двумя уполномоченными сотрудниками службы ДОУ, а также представителем отдела средств технической защиты. Такой состав проверяющей ко-

миссии из специалистов по разным типам носителей информации повышает качество проверок и ускоряет их проведение.

Конечные результаты проверок фиксируются в актах. В случае выявления фактов утраты документов или их отсутствия без соответствующей записи в журнале учета выдачи документов должны быть приняты меры по их устранению.

Мнение эксперта



И.В. Баранова,
руководитель секретариата холдинговой компании

Хотелось бы отметить, что количество потенциальных каналов утечки конфиденциальной информации в организации достаточно велико даже при наличии документа, который регламентирует работу в организации с конфиденциальной информацией.

Наиболее распространенный из них относится к категории неумышленного раскрытия информации сотрудниками по причине неосведомленности или недисциплинированности.

У большинства сотрудников отсутствуют представления о правилах работы с конфиденциальными документами и умение определить, какие документы конфиденциальны. Порой обычные разговоры между сотрудниками приводят к рассекречиванию конфиденциальных данных.

В большинстве случаев проблему утечки нельзя решить простым способом или избавиться от нее окончательно. Необходимо разработать систему организационно-технических мероприятий, позволяющих перекрыть основные каналы утечки информации с определенной степенью надежности.

Система будет включать основные составляющие: работу с персоналом, политику безопасности, сервисы безопасности.

Как показывает практика, значительного ограничения утечки информации из организации можно добиться путем применения следующих правил, которым в обязательном порядке должны следовать сотрудники организации:

1. Идентификация (маркирование) документов, содержащих конфиденциальную информацию.

2. Закрытое обсуждение – не допускать обсуждения конфиденциальной информации с посторонними лицами или в их присутствии.

3. Электронный обмен конфиденциальной информацией с внешними респондентами должен вестись в зашифрованном виде (при наличии соответствующих технических возможностей).

4. Заключение соглашения о конфиденциальности – передача конфиденциальной информации третьей стороне только при условии заключенного соглашения.

5. Ограничение доступа к информации – документы, содержащие конфиденциальную информацию нельзя хранить в общедоступных местах, включая общие папки файловых серверов, почтовые папки, web и др.

6. Информирование сотрудников – ведение разъяснительной работы с сотрудниками о методах защиты информации, а также контроль ее выполнения. Сообщение обо всех фактах утечки непосредственному руководителю.

Также необходимо проводить аудиты информационной безопасности для оперативного обнаружения и реагирования на нарушения безопасности.

В случае если принятые меры не привели к положительным результатам, приказом по организации создается специальная комиссия для установления причин отсутствия документов (носителей) и проведения их поиска.

При любом исходе комиссия должна составить заключение о результатах своей работы, выявить причины отсутствия документов, предложить пути решения по устранению этих причин, установить степень вины конкретных сотрудников.

При ликвидации предприятия проверка наличия носителей, документов, дел, регистрационных форм проводится комиссией, назначаемой руководителем предприятия. Результаты проверки оформляются актом, который приобщается к общему акту о ликвидации.

Формы организации конфиденциального делопроизводства

Безусловно, журнально-карточные формы организации конфиденциального делопроизводства зарекомендовали себя давно, прошли проверку десятилетиями. Наиболее известна **журнальная форма** ведения делопроизводства – вся информация в журналы заносится от руки. Журналы занимают мало места в сейфах, их сохранность не требует дополнительных затрат.

№ п/п	Дата регистрации документа	Корреспондент	Исходящий номер документа	Дата	Краткое содержание	Листаж	Кол-во экземпляров
1	2	3	4	5	6	7	8

Продолжение

Кому (название подразделения и Ф.И.О. исполнителя)	Резолюция (№ , дата, содержание)	Отметка об исполнении	Расписка в получении		Примечание
			Дата	Подпись	
9	10	11	12	13	14

1. **№ п/п** – проставляется порядковый регистрационный номер входящего документа.

2. **Дата регистрации документа** – текущая дата регистрации.

3. **Корреспондент** – наименование корреспондента – организации, являющейся автором документа или его отправителем.

4. **Исходящий номер документа** – номер, присвоенный документу корреспондентом. Если исходящий номер не присвоен, указываем «б/н» (т. е. без номера).

5. **Дата** – исходящая дата документа: заносится дата, присвоенная корреспондентом-отправителем, если даты нет, проставляем «б/д» (т. е. без даты).

6. **Краткое содержание** – тема данного документа.

7. **Листаж** – фиксируется полный листаж документа и приложений (если таковые есть).

8. **Кол-во экземпляров** – указывается количество экземпляров, если их несколько. Если документ прислан в единственном экземпляре – в этой графе ставится прочерк.

9. **Кому** – указывается название подразделения, в которое направляется документ, и Ф.И.О. исполнителя документа. Если исполнитель неизвестен, указывается Ф.И.О. руководителя подразделения, в которое направлен документ.

10. **Резолюция** – резолюция руководства. Если в организации ведется регистрация резолюций, указывается присвоенный резолюции учетный номер.

11. **Отметка об исполнении** – вносится краткая запись по решению вопроса.

12, 13. **Расписка в получении.** Дата, подпись – документ всегда передается исполнителю под роспись. Дата передачи проставляется в обязательном порядке.

14. **Примечание** – в данной графе целесообразно проставлять отметки об уничтожении (Уничтожено, акт № __ от _____), о подшивке документа в дело (В дело № ___ год___), о передаче дела на архивное хранение (Опись дел № ____ от ____), об утрате документа (Акт № ____ от _____).

Карточная форма ведения делопроизводства более эффективна в учреждениях с большим объемом документооборота. При разработке карточки можно взять за основу стандартную форму простой регистрационной карточки, но добавить в нее поля согласно специфике конфиденциального делопроизводства:

«Гриф», «Категория», «Листаж документа», «Отметка об уничтожении», графа «Расписка в получении» здесь имеет статус «обязательна к заполнению».

Электронная форма ведения делопроизводства – конечно, наиболее затратная, но и наиболее эффективная. Сегодня на рынке есть множество программных продуктов, предлагающих свои решения в области ведения общего и конфиденциального делопроизводства. Совершенных решений нет. При выборе системы электронного документооборота руководство предприятия должно привлечь экспертов из служб технической защиты информации, которые определят комплекс программно-аппаратных средств защиты информации. Программное обеспечение должно быть лицензировано. Компьютеры, на которых будет установлен выбранный программный продукт, должны быть подключены только к защищенной локальной сети и ни к каким другим сетям, не иметь выхода в Интернет. Также эти компьютеры, помимо аппаратных средств защиты, должны иметь хорошую программную защиту, а каждый сотрудник, работающий в локальной сети, –

иметь свой уникальный пароль, за регулярным обновлением которых следит служба технической поддержки системы.

Какую форму ведения делопроизводства внедрять на предприятии – решение всегда остается за руководителями.

Приложение

ОБЯЗАТЕЛЬСТВО О НЕРАЗГЛАШЕНИИ

Я, _____,

(фамилия, имя, отчество, должность)

в качестве работника ООО «Ромашка» в период трудовых отношений с предприятием и по их окончании обязуюсь:

1. Не разглашать сведения конфиденциального характера, в том числе информацию, составляющую коммерческую тайну, которые мне будут доверены или станут известны по работе.

2. Не передавать третьим лицам и не раскрывать публично конфиденциальную информацию без согласия руководства ООО «Ромашка».

3. Выполнять относящиеся ко мне требования приказов, инструкций и положений по обеспечению конфиденциальности информации.

4. В случае попытки посторонних лиц получать от меня конфиденциальную информацию немедленно сообщить своему непосредственному руководителю и представителю Департамента безопасности.

5. Сохранять конфиденциальность информации тех предприятий, с которыми ООО «Ромашка» имеет деловые отношения.

6. Не использовать знания информации, составляющей коммерческую тайну предприятия, для занятия любой другой деятельностью, которая может нанести ущерб ООО «Ромашка».

7. Не передавать конфиденциальную информацию в общедоступные информационные среды (Интернет) без получения соответствующего разрешения Директора по безопасности.

8. В случае моего увольнения все носители информации (рукописи, черновики, чертежи, магнитные ленты, диски, дискеты, распечатки с принтеров, кино-, фотонегативы и позитивы, модели, материалы, изделия и пр.), которые находились в моем распоряжении в связи с выполнением мною служебных обязанностей во время работы в ООО «Ромашка», передать моему непосредственному руководителю или лицу, его замещающему.

9. Об утрате или недостаче носителей конфиденциальной информации, удостоверений, пропусков, ключей от режимных помещений, хранилищ, сейфов (металлических шкафов), личных печатей и других фактах, которые могут привести к разглашению конфиденциальной информации, а также о причинах и условиях возможного разглашения информации немедленно сообщать моему непосредственному руководителю или лицу, его замещающему, и представителю Департамента безопасности.

Я поставлен в известность о том, что нарушение этого обязательства может повлечь за собой ответственность, предусмотренную действующим законодательством, включая административную и уголовную ответственность.

_____

(подпись)

«___»_____20____г.

Один экземпляр обязательства получил

_____

(подпись)

«___»_____20____г.