Организация работы с конфиденциальной информацией

I. ВВЕДЕНИЕ

Перечень основных законодательных и других нормативных актов, регламентирующих работу с конфиденциальной информацией:

1. Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 11.07.2011) "О коммерческой тайне"

2. "Гражданский кодекс Российской Федерации (часть четвертая)" от 18.12.2006 N 230-ФЗ (ред. от 23.07.2013) (с изм. и доп., вступающими в силу с 01.09.2013)
   Статья 1465. Секрет производства (ноу-хау)

3. Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ (принят ГД ФС РФ 21.12.2001) (ред. от 02.04.2014) (с изм. и доп., вступающими в силу с 13.04.2014)

4. Постановление Правительства РСФСР от 05.12.1991 N 35 (ред. от 03.10.2002) "О перечне сведений, которые не могут составлять коммерческую тайну"

5. Федеральный закон от 29.11.2001 N 156-ФЗ (ред. от 22.04.2010) "Об инвестиционных фондах" (принят ГД ФС РФ 11.10.2001)
   Статья 56. Ответственность федерального органа исполнительной власти по рынку ценных бумаг за соблюдение коммерческой тайны

6. Федеральный закон от 11.11.2003 N 152-ФЗ (ред. от 09.03.2010) "Об ипотечных ценных бумагах" (принят ГД ФС РФ 14.10.2003)
   Статья 44. Ответственность федерального органа исполнительной власти по рынку ценных бумаг за соблюдение коммерческой тайны

7. Федеральный закон "Об инвестиционных фондах"
   Статья 56. Ответственность федерального органа исполнительной власти по рынку ценных бумаг за соблюдение коммерческой тайны

8. Уголовный кодекс Российской Федерации
   Статья 17.2. Обязанность органов, уполномоченных на осуществление контроля в сфере размещения заказов, по соблюдению государственной, коммерческой, служебной, иной охраняемой законом тайны
   Статья 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (п.3. до пяти лет лишения свободы)

9. Федеральный закон от 26 июля 2006 г. N 135-ФЗ "О защите конкуренции" Статья 26. Обязанность антимонопольного органа по соблюдению коммерческой, служебной, иной охраняемой законом тайны

10. Указ Президента РФ от 06.03.1997 N 188 "Об утверждении Перечня сведений конфиденциального характера"

11. Конституция РФ 1993 г. (ст. 34)

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

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;

(ст. 3, Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне" (принят ГД ФС РФ 09.07.2004))

Под информацией, составляющей коммерческую тайну, в соответствии с указанным Законом 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 ст.5 данного Закона приведен перечень сведений, которые не могут составлять коммерческую тайну:

1) содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;

3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

5) о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

6) о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

7) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

9) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

11) обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

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 документов, содержащих коммерческую тайну, и закрепленных на бумажных носителях. Средства технической защиты в данной статье не рассматриваются.

II. 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 введении 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.
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.
Если в организации отсутствует служба ДОУ/Секретариат, необходимо создать такое подразделение, а также определить специалистов технической службы и службы безопасности, которые будут отвечать за обеспечение защиты конфиденциальной информации от конкурентов и пр. рисков.

Мы рекомендуем при разработке «Положения о конфиденциальной информации», включить следующие разделы:

1. Общие положения.
   В данном разделе нужно кратко описать предназначение данного документа, раскрыть основные понятия (конфиденциальная информация), дать ссылку на федеральные законы.
2. Правила категорирования конфиденциальной информации.
   Российское законодательство предоставляем коммерческим организациям возможность использовать только один гриф «Коммерческая тайна», что не всегда удобно. Да, коммерческие организации не могут использовать даже гриф «ДСП» (для служебного пользования). Но такие жесткие рамки не всегда удобны в работе. Поэтому можно ввести такое понятие, как «Категорирование информации», т.е. когда документам, выпускаемым под грифом «Коммерческая тайна», мы можем присваивать некие дополнительные

категории, позволяющие внутри организации разграничивать, например, степень допуска сотрудников к данным документам, порядок обработки документов с той или иной категорией.

3. Защита информации.
   В данном разделе перечисляются меры, принимаемые в организации для защиты информации: определения 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, хранения, уничтожения данной информации.
4. 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 перечисляем условия, при наступлении которых доступ сотрудников к данной информации может быть прекращен.
5. 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, 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.
6. Защита конфиденциальной информации в процессе служебной деятельности.
   Оговаривается обязательность защиты сведений, составляющих коммерческую тайну, и ответственность сотрудников, получивших доступ к данной информации. Также оговаривается порядок обращения с данными документами, условия их хранения, передачи, перевозки, порядок действия при наступлении форс-мажорных обстоятельств.
7. 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.

8. 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 тайн», необходимо помимо пунктов, включенных в простую Инструкцию по делопроизводству, включить следующие положения:

- порядок выноса-вноса конфиденциальных документов применительно к 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 в отпуск, командировку или увольнение с работы;
- порядок подготовки конфиденциальных документов, его 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» все сотрудники организации должны быть ознакомлены с данным документом под расписку.
И каждый сотрудник должен подписать «Обязательство о неразглашении коммерческой тайны, ставшей известной в период работы в данной организации». Все вновь пришедшие в организацию работники, должны подписывать такой документ при приеме на работу, после ознакомления с «Положением..».
Стандартный текст «Обязательства о неразглашении» - см. в Приложении № 1.

III. Централизованная и смешанная форма ведения конфиденциального делопроизводства

При любой форме организации 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 учреждения 1-й категории (более 1000 сотрудников, большой объем 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 др.типах носителей информации. А также подразделения технической защиты информации.

В учреждениях с небольшими объемами документов, содержащих коммерческую тайну, остаются те же функции, но требуют участия в обработке документов гораздо меньшего количества сотрудников.

Конфиденциальное делопроизводство базируется на тех же принципах, что и простое, но отличается большим количеством видов работ, которые начинаются с момента создания документа, что требует четкого механизма учета черновиков, учета копий документов, документирования уничтожения всех видов носителей информации, контроль за исполнением документов, контроль за отправкой, систематизацией, за соблюдением режима хранения, обращения к документам, за подготовкой и передачей на архивное хранение. Плюс еще одна составляющая – защита информации, содержащейся в документах: подразделение средств технической защиты информации, например криптографической.

IV. Требования к служебным помещениям

Служебное помещение должно обеспечивать необходимую площадь на каждое рабочее место, быть оснащено прочной удобной мебелью, оснащено средствами орг.техники (если необходимо). Помещения для работы с документами, составляющими коммерческую тайну, предназначенные для круглосуточного хранения документов, в целях обеспечения дополнительных гарантий от постороннего проникновения в них не должны находиться на первом и последнем этажах. Кроме того, они должны соответствовать нормам, установленным для хранения документов, удалены от помещений с пищевыми продуктами и химическими веществами, не иметь с ними общих вентиляционных каналов, отвечать требованиям пожарной безопасности, санитарным нормам, а также быть гарантированными от затопления.

Вход в такие помещения необходимо строго регламентировать. Кроме руководителя предприятия и сотрудников, имеющих прямое отношение к обработке и хранению документов, составляющих коммерческую тайну, в помещения должны допускаться люди, обеспечивающие их обслуживание: уборщицы, персонал, обеспечивающий ремонт и обслуживание оборудования и средств орг.техники. Любые работы, производящиеся в помещениях, где хранятся конфиденциальные документы, должны производиться в присутствии сотрудников, в чьем ведении в данный момент находятся документы, содержащие коммерческую тайну.

Окна помещений должны быть снабжены средствами защиты (сигнализацией, жалюзи, железной сеткой), исключающих возможность проникновения в помещения посторонних лиц, а также возможность визуального просмотра документов и мониторов с улицы. Рядом с помещениями не должны находиться пожарные лестницы, балконы, водосточные трубы. Входные двери должны быть обиты металлом и оборудованы надежными дверными замками. По окончании рабочего дня двери должны запираться на замки и опломбироваться. Перед открытием двери необходимо проверять на предмет целостности печатей. Для предотвращения несанкционированного входа в течение дня двери должны оборудоваться электромеханическими или электронными замками. Входные двери должны быть также оснащены сигнализацией.

Орг.техника: средства для размножения, создания, изготовления документов, быстрого их поиска. Для сохранности документов необходимо наличие несгораемых шкафов (сейфов). Помимо обычных классических сейфов хорошо зарекомендовали себя также roller-shelves: подвижные сейфы на рельсах, которые "складываются гармошкой» и занимают меньше места в обычном состоянии. И легко «раскладываются» и обеспечивают доступ сотрудников к нужным документам.

Помещения, в которых используются электронные средства орг.техники: компьютеры, копировальные аппараты, средства аудио-, видеозаписывающей техники, воспроизводящей электромагнитные излучения, должны быть оборудованы дополнительными средствами защиты, предотвращающими перехват электронных сигналов. Средства защиты необходимо приобретать только сертифицированные, а средства иностранного производства в обязательном порядке подвергать предварительной спецпроверке.

V. Организация работы службы сейфово-ключного хозяйства

Необходимо организовать учет ключей и металлических печатей для опечатывания сейфов и комнат, которые выдаются сотрудникам. К каждому сейфу в комплекте предприятие-изготовитель прилагает три ключа: один ключ выдается сотруднику, запасные экземпляры, хранятся в подразделении, отвечающем за ключное хозяйство. В таких подразделениях обычно превалирует журнальная форма учета выдачи ключей и печатей или заводятся карточки лицевого счета. Для обеспечения максимальной безопасности работы с документами необходимо, чтобы все сотрудники, имеющие доступ к документам, составляющих коммерческую тайну, имели на рабочих местах сейфы.

Такие сейфы в обязательном порядке должны не только закрываться на ключ, но и опломбироваться (мастика, нить, металлическая печать). После опломбирования сейфа сотрудник обязан также опломбировать помещение (если уходит последним) убрать ключи в специальный пенал, опломбировать его. Каждый пенал должен иметь свой номер. Опломбированные пеналы должны сдаваться на пост охраны предприятия под расписку в журнале. В этом случае у сотрудников

службы охраны предприятия должен быть список сотрудников, имеющих право на сдачу-получение пронумерованных пеналов с ключами. С учетом специфики подразделения, не следует слишком доверять электронным замкам. Возможно использование и тех и других видов замков. Важно, чтобы сотрудники, имеющие доступ к документам, составляющим коммерческую тайну, не носили с собой ключей в карманах и сумках. При таком подходе к процессу мы увеличиваем риски утечки информации. Да и банальный страх потери ключей, от которой никто не застрахован, может постоянно действовать на нервы сотрудникам. Правильный вариант – на связке ключей сотрудника должна быть только металлическая печатка, никаких ключей от сейфов.

Помещение также должно быть оснащено техническими средствами защиты информации: термодатчиками, средствами видеонаблюдения, и пр. Также необходимы средства для создания помех прослушивания и просмотра информации извне.

В помещениях, предназначенных для хранения конфиденциальных документов, должно находиться достаточное количество тары: спецконтейнеров, мешков, ящиков, в которых можно транспортировать документы.

Место для эвакуации документов должно быть определено заранее, о нем должны знать сотрудники службы ДОУ и службы охраны.

VI. **Формы организации конфиденциального делопроизводства**:

Журнальная, Карточная, Электронная.

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.

При *карточной форме* ведения делопроизводства процесс будет стоить несколько дороже: разработка и заказ в типографии форм учетных карточек. Но карточная форма ведения делопроизводства более эффективна в учреждениях с б*о*льшим объемом документооборота.

Электронная форма ведения делопроизводства – конечно, наиболее затратная, но и наиболее эффективная. Сегодня на рынке существует 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 комплект программно-аппаратных средств защиты информации. Программное обеспечение должно быть лицензировано. Компьютеры, на которых будет установлен выбранный программный продукт, должны быть подключены к

защищенной локальной сети и не должны быть подключены 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, должен иметь свой уникальный пароль, за регулярным обновлением которых должна следить служба технической поддержки системы. Преимущества данной системы – моментальный доступ к информации, сокращение в десятки раз времени на обработку информации. Формирование отчетов происходит за несколько секунд. Контроль исполнения (сроковый) ведется автоматически. Полный контроль за жизненным циклом документов и обращениям к ним.

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

Приложение № 1

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 деятельностью, которая в качестве конкурентного действия 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 заменяющему.
9. Об утрате или недостаче носителей конфиденциальной информации, удостоверений, пропусков, ключей от режимных помещений, хранилищ, сейфов (металлических шкафов), личных печатей и о 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.

Один экземпляр обязательства получил

_____ _____

(подпись) (подпись)

"___"_____200____г. "___"_____200____г.