Лекция 2. Конфиденциальное делопроизводство

Вопросы:

2.1.Перечень сведений конфиденциального характера

2.2. Формирование системы защиты конфиденциальных документов.

2.3. Жизненный цикл конфиденциального документа.

2.1.Перечень сведений конфиденциального характера

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

2. Сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20 августа 2004 года N 119-ФЗ "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства" и другими нормативными правовыми актами Российской Федерации (пункт дополнен Указом Президента Российской Федерации от 23 сентября 2005 года N 1111 - см. предыдущую редакцию).

Указ Президента РФ от 6.03.1997 г. №188
(изменения внесены Указом Президента РФ от 23.09.2005 г. №1111)

Перечень сведений конфиденциального характера (окончание)

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).
4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).
5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).
6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Документы, содержащие сведения, которые составляют негосударственную тайну (служебную, коммерческую, банковскую, тайну фирмы и др.) или содержат персональные данные, именуются **конфиденциальными.**

Информация, как правило, содержащаяся в конфиденциальных документах

- техническая, технологическая: методы изготовления продукции, программное обеспечение, производственные показатели, химические формулы, результаты испытаний опытных образцов, данные контроля качества и т. п.;
- деловая: стоимостные показатели, результаты исследования рынка, списки клиентов, экономические прогнозы, стратегия действий на рынке и т. п.
- корпоративная: отдельные виды инструкций, регламентов, данные о персонале и т.п.

2.1. Формирование системы защиты конфиденциальных документов

1 Этап. Выявление и регламентация конфиденциальной информации

Выявление и регламентация реального состава информации, представляющей ценность для предпринимателя и составляющей тайну фирмы, – основополагающие части системы защиты информации.

Состав ценной информации фиксируется в специальном **перечне,** определяющем **срок** и **уровень** (гриф) ее конфиденциальности (то есть недоступности для всех), **список сотрудников фирмы**, которым предоставлено право использовать эти сведения в работе.

Перечень сведений, отнесенных к конфиденциальным в ООО «….

Тип сведений	Гриф	Срок действия	Кто допущен
Техническая и технологическая информация			
Содержание технических заданий на разработку новых образцов	СК	до окончания проекта	Ген.директор, Глав.инженер
Деловая информация			
Содержание договоров с инвесторами	СК	определяется договором	Ген.директор, Ком.директор
Объем инвестиций на текущий год	К	до окончания финансового года	Ген.директор, фин.директор
Корпоративная информация			
Данные по персоналу	ДСП	постоянно	Ген.директор, начальник ОК

Конфиденциальность отражает ограничение, которое накладывает собственник информации на доступ к ней других лиц, то есть собственник устанавливает правовой режим этой информации в соответствии с законом.

Называть конфиденциальные документы секретными или ставить на них гриф секретности не допускается.

Особенностью конфиденциального документа является то, что он одновременно представляет собой:

- массовый носитель ценной, защищаемой информации;
- основной источник накопления и объективного распространения этой информации, а также ее неправомерного разглашения или утечки;
- обязательный объект защиты.

Конфиденциальные документы, как и открытые, находятся в постоянном движении во времени и пространстве, что отражает их объективную сущность как носителя информации, необходимой руководителям и сотрудникам фирмы для выполнения функциональных обязанностей и принятия решений.

Принципы и направления движения конфиденциальных традиционных и электронных документов в аппарате управления фирмы **едины при использовании любой технологической системы обработки и хранения документов. Методы работы с** документами меняются, но технологическая взаимосвязь документооборота с процессом управления сохраняется.

Перемещение конфиденциальных документов (КД) по множеству иерархических уровней управления создает серьезные предпосылки **потенциальные возможности (угрозы)** для утраты ценной информации, требует осуществления защитных мер в отношении документопотоков и документооборота в целом.

2 Этап. Определение угроз

- **кража (хищение) документа или отдельных его частей** (листов, приложений, копий, схем, фотографий и др.), носителя чернового варианта документа или рабочих записей;
- **несанкционированное копирование** бумажных и электронных документов, баз данных, фото-, видео- и аудиодокументов, запоминание злоумышленником или его сообщником текста документа;
- **тайное или разрешенное ознакомление сотрудника фирмы** с документом и **сообщение информации злоумышленнику** лично или по линиям связи, прочтение текста документа по телефону или переговорному устройству, разглашение информации с помощью мимики, жестов, условных сигналов;
- **подмена документов**, носителей и их отдельных частей с целью фальсификации или сокрытия факта утери, хищения;
- **дистанционный просмотр документов и изображений дисплея** с помощью технических средств визуальной разведки;

- **ошибочные (умышленные или случайные) действия** персонала при работе с документами (нарушение разрешительной системы доступа, правил обращения с документами, технологии их обработки и хранения);
- **случайное или умышленное уничтожение** ценных документов и баз данных;
- **несанкционированная модификация и искажение** текста, реквизитов;
- **считывание данных в чужих массивах** за счет использования остаточной информации на копировальной ленте, бумаге, дисках и дискетах;
- **утечка информации** по техническим каналам при обсуждении и диктовке текста документа, работе с компьютером и другой офисной техникой;
- **гибель документов** в условиях экстремальных ситуаций.

Дополнительные угрозы для электронных документов

- **непреднамеренные ошибки пользователей,** операторов, референтов, управляющих делами, работников службы конфиденциальной документации (далее – службы КД), системных администраторов и других лиц, обслуживающих информационные системы (самая частая и большая опасность);
- **кражи и подлоги** информации;
- **угрозы, исходящие от стихийных ситуаций** внешней среды;
- **угрозы заражения вирусами**.

Под **защищенным документооборотом (документопотоком)** понимается контролируемое движение конфиденциальной документированной информации по регламентированным пунктам приема, обработки, рассмотрения, исполнения, использования и хранения в жестких условиях организационного и технологического обеспечения безопасности как носителя информации, так и самой информации.

Помимо общих для документооборота принципов защищенный документооборот основывается на ряде дополнительных принципов:

3. Этап. Определение принципов КД

- **ограничение доступа персонала к документам**, делам и базам данных деловой, служебной или производственной необходимостью;
- **персональная ответственность должностных лиц** за выдачу разрешения на доступ сотрудников к конфиденциальным сведениям и документам;
- **персональная ответственность каждого сотрудника** за сохранность доверенного ему носителя и конфиденциальность информации;
- **жесткая регламентация порядка работы с документами,** делами и базами данных **для всех категорий персонала**, в том числе **первых руководителей.**

Защищенность КД достигается за счет:

- **одновременного использования режимных** (разрешительных, ограничительных) мер и **технологических приемов,** входящих в систему обработки и хранения конфиденциальных документов;
- нанесения **отличительной отметки (грифа) на чистый носитель конфиденциальной информации** или документ, в том числе сопроводительный, что позволяет выделить их в общем потоке документов;

Защищенность КД достигается за счет:

- формирования **самостоятельных, изолированных потоков** конфиденциальных документов и (часто) дополнительного их разделения на подпотоки в соответствии с уровнем конфиденциальности перемещаемых документов;
- использования **автономной технологической системы** обработки и хранения конфиденциальных документов, **не соприкасающейся** с системой обработки открытых документов.

2.3. Жизненный цикл конфиденциального документа

Под **исполнением** конфиденциального документа понимается процесс документирования:

- управленческих решений;
- действий, результатов выполнения руководителями и сотрудниками фирмы поставленных задач и отдельных заданий, поручений;
- реализации функций, закрепленных за ними в должностных инструкциях.

Факторами, инициирующими процесс исполнения, являются:

Факторы, инициирующие процесс исполнения КД

- получение руководителем, сотрудником (исполнителем) поступившего документа;
- письменное или устное указание вышестоящего руководителя;
- устный запрос на информацию или принятие решения от других фирм, учреждений и отдельных лиц;
- задания и поручения, включенные в рабочие планы, графики работы, должностные инструкции и другие организационные и плановые документы;
- полезная информация, полученная из реферативных и информационных сборников, рекламных изданий.

В отличие от исполнения открытых документов исполнение конфиденциальных документов представляет собой стадию, насыщенную различными технологическими этапами и процедурами, основными из которых являются:

- **установление уровня грифа конфиденциальности** сведений, подлежащих включению в будущий документ (на основе перечня сведений);
- **оформление и учет носителя** для документирования выделенного комплекса конфиденциальной информации (на основе перечня документов);
- **составление и изготовление** проекта конфиденциального документа;
- **издание конфиденциального** документа.

2.3.1. Установление грифа конфиденциальности

Своевременное **установление грифа конфиденциальности** сведений, подлежащих включению в будущий документ, – первый и **основной элемент защиты** документированной информации, позволяющий обеспечить относительно надежную безопасность тайны фирмы.

Основу присвоения документу грифа конфиденциальности должны составлять:

- перечень конфиденциальных сведений фирмы;
- требования партнеров;
- перечень конфиденциальных документов фирмы.

Система грифования документов не гарантирует сохранности информации, однако позволяет четко организовать работу с документами, в частности сформировать систему доступа к документам персонала.

Гриф конфиденциальности, или гриф ограничения доступа к традиционному, машиночитаемому или электронному документу, представляет собой реквизит (элемент, служебную отметку, помету) формуляра документа, свидетельствующий о конфиденциальности содержащихся в документе сведений и проставляемый на самом документе и (или) сопроводительном письме к нему.

Информация и документы, отнесенные к коммерческой (предпринимательской) тайне, имеют несколько уровней грифа ограничения доступа, соответствующих различным степеням конфиденциальности информации:

- первый, массовый уровень – грифы «Конфиденциально», «Конфиденциальная информация»;
- второй уровень (достаточно редкий) – грифы «Строго конфиденциально», «Строго конфиденциальная информация», «Особый контроль» – они присваиваются документу лично первым руководителем фирмы, им изменяются или отменяются. Использование и хранение этих документов также организуется первым руководителем с возможным привлечением руководителя службы КД;
- на документах, содержащих сведения, отнесенные к служебной тайне, ставится гриф «Для служебного пользования» («ДСП»).

Гриф ограничения доступа на документе пишется полностью, то есть не сокращается. Под обозначением грифа указываются номер экземпляра документа, срок действия грифа и иные условия его снятия.

Обычно гриф располагается на первом и титульном листах документа, а также на обложке дела (тома) в правом верхнем углу. На электронных документах и документах, записанных на любых машинных носителях, гриф обозначается на всех листах.

Ниже грифа или ниже адресата могут обозначаться ограничительные пометы: «Лично», «Только в руки», «Только адресату», «Лично в руки» и др.

При регистрации конфиденциального документа к его номеру добавляется сокращенное обозначение грифа конфиденциальности.

Размещение грифа конфиденциальности

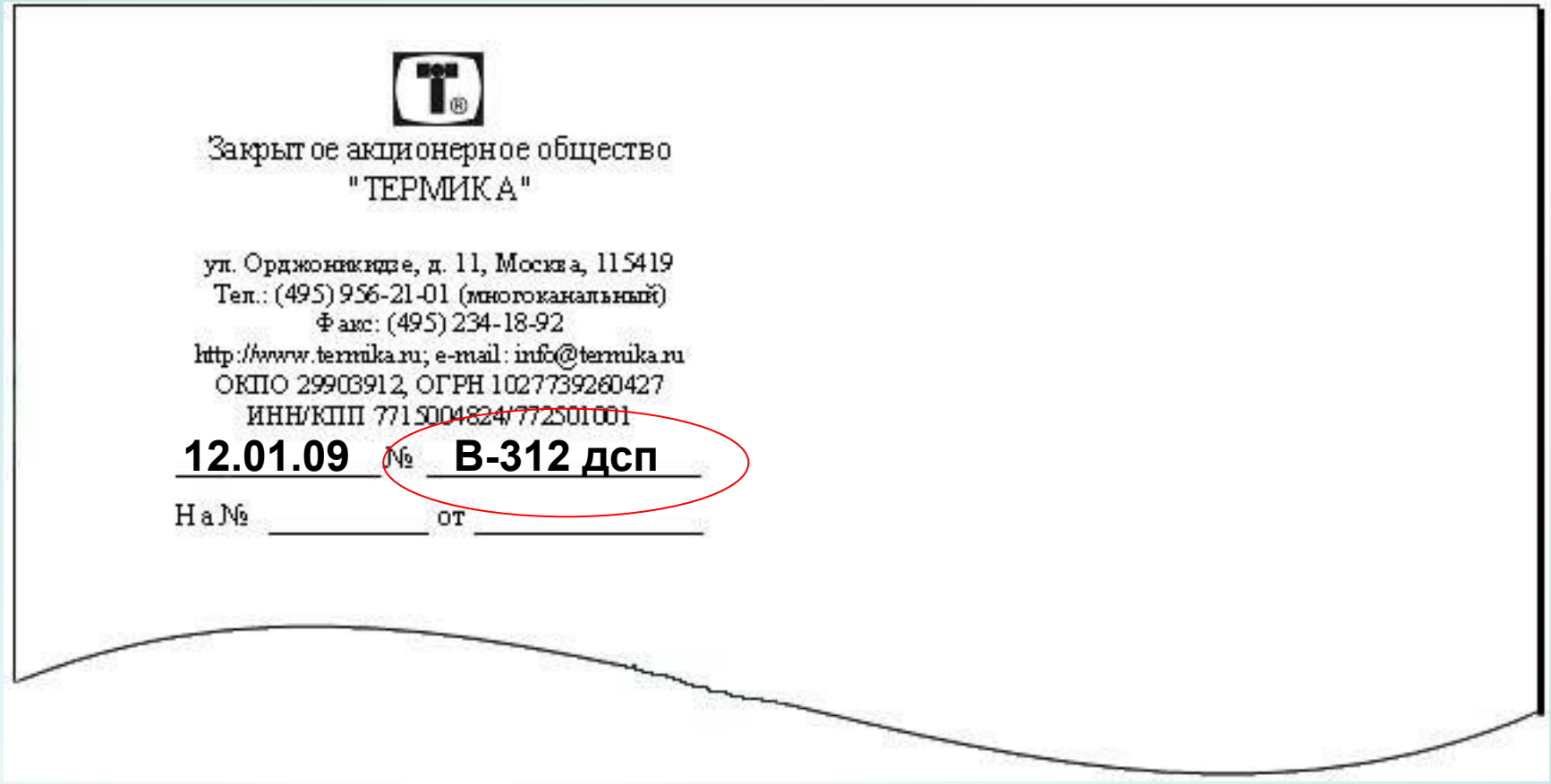
Конфиденциально
Экз.№1

ПЛАН
инвестиций ООО «…..» на 2009 г.

Строго
конфиденциально
Экз.№1

СВЕДЕНИЯ
о перспективных образцах продукции

Размещение грифа конфиденциальности



Закрытое акционерное общество
"ТЕРМИКА"

ул. Орджоникидзе, д. 11, Москва, 115419
Тел.: (495) 956-21-01 (многоканальный)
Факс: (495) 234-18-92
http://www.termika.ru; e-mail: info@termika.ru
ОКПО 29903912, ОГРН 1027739260427
ИНН/КПП 7715004824/772501001

12.01.09 № **В-312 дсп**

На № _____ от _____

При присвоении грифа конфиденциальности документа необходимо помнить:

- гриф конфиденциальности определяется **исполнителем** документа;
- гриф конфиденциальности документа присваивается по **наивысшей** степени конфиденциальности сведений, изложенных в нём.

2.3.2. Оформление и учет носителя для документирования выделенного комплекса конфиденциальной информации

- Подготовка бумажных носителей с соответствующим грифом конфиденциальности (бланки строгой отчетности);
- Определение перечня вычислительной техники (в том числе съемных носителей информации), на которой допускается разработка и хранение конфиденциальных документов;
- Выдача (под роспись) бумажных носителей исполнителям;
- Закрепление вычислительной техники за исполнителями, допущенными к разработке конфиденциальных документов.

2.3.3. Составление и изготовление проекта конфиденциального документа;

1.7. Жизненный цикл документа

В целом жизненный цикл (движение) исходящих документов включает следующие этапы:

1. Подготовка исполнителем проекта документа.
2. Согласование (визирование) проекта документа.
3. Доработка проекта документа по замечаниям.
4. Повторное визирование документа.
5. Подписание документа руководителем.
6. Регистрация документа (в службе ДОУ или в подразделении, если документ подписан руководителем подразделения).
7. Передача документа в службу ДОУ (если документ подписан руководителем подразделения).
8. Отправка документа корреспонденту и передача копии в дело.

В ходе исполнения конфиденциальных документов могут возникнуть следующие основные угрозы:

- **утрата (разглашение, утечка)** ценной информации за счет ее документирования на случайном носителе, не входящем в сферу контроля службы конфиденциальных документов (КД);
- **подготовка к изданию документа, не обоснованного деловой необходимостью или не разрешенного** для издания, то есть документирования определенной информации;
- **включение в документ избыточных конфиденциальных** сведений, что равносильно разглашению тайны фирмы;
- **случайное или умышленное занижение грифа конфиденциальности** сведений, включенных в документ;

- изготовление документа в **условиях, которые не гарантируют сохранности носителя**, конфиденциальности информации;
- **утеря оригинала, черновика, варианта или редакции документа, его части,** приложения к документу, **умолчание** этого факта и **попытка подмены** утраченных материалов;
- **сообщение** содержания проекта конфиденциального или открытого документа **постороннему лицу**, несанкционированное копирование документа или его части (в том числе на неучтенной дискете);
- **утечка** информации по техническим каналам;
- **ошибочные действия работника службы КД**, особенно в части нарушения разрешительной системы доступа к документам.

2.3.4. Издание конфиденциального документа.

1.7. Жизненный цикл документа

В целом жизненный цикл (движение) исходящих документов включает следующие этапы:

1. Подготовка исполнителем проекта документа.
2. Согласование (визирование) проекта документа.
3. Доработка проекта документа по замечаниям.
4. Повторное визирование документа.
5. Подписание документа руководителем.
6. Регистрация документа (в службе ДОУ или в подразделении, если документ подписан руководителем подразделения).
7. Передача документа в службу ДОУ (если документ подписан руководителем подразделения).
8. Отправка документа корреспонденту и передача копии в дело.

Использование конфиденциальных документов

В отличие от исполнения процесс **использования** документа предполагает включение его в информационно-документационную систему, обеспечивающую исполнение других документов, выполнение управленческих действий и решений.

Для использования в работе обычно поступают законодательные акты, организационно-правовые, нормативные, распорядительные, справочно-информационные документы, разнообразные рекламные издания и научно-техническая информация.

Процесс ознакомления с конфиденциальным документом – это информирование сотрудника фирмы или иного заинтересованного лица, осуществляемое в соответствии с резолюцией полномочного руководителя на конфиденциальном документе, о принятом этим руководителем решении или решении другой организационной структуры.