Лекция 2. Требования к оформлению конфиденциальных документов

2.1. Требования к оформлению КД.

2.2. Структура защищаемых документопотоков, состав технологических этапов и операций.

2.3. Технологические системы защиты и обработки КД.

2.1. Требования к оформлению конфиденциальных документов

Под конфиденциальным документом понимается необходимым образом оформленный носитель документированной информации, содержащей сведения ограниченного доступа или использования, которые составляют интеллектуальную собственность юридического или физического лица.

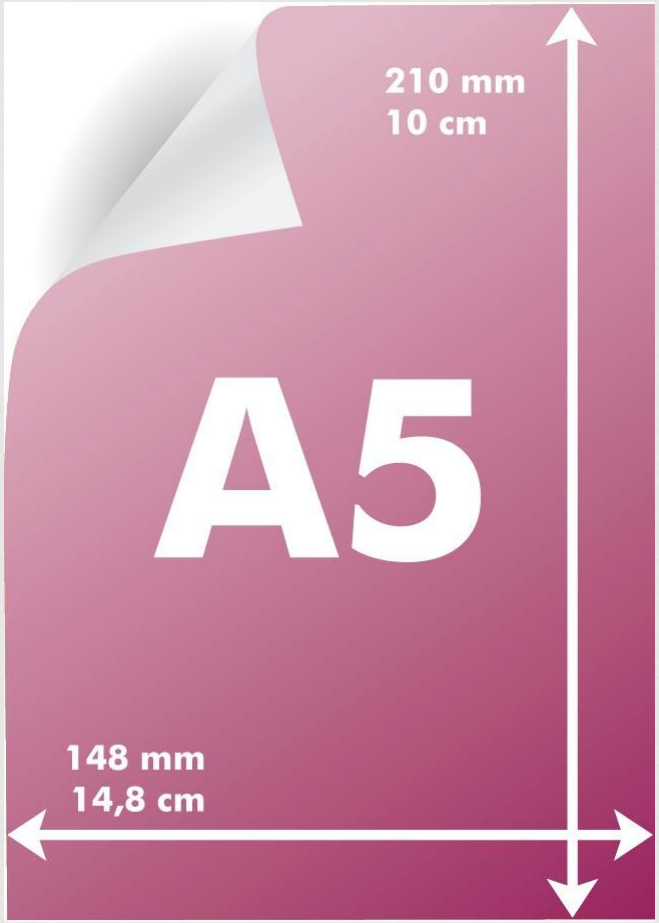
Чтобы КД имел юридическую силу, он должен быть должным образом оформлен, т. е. иметь соответствующие реквизиты.

Для организационно-распорядительных документов (ОРД) состав реквизитов и правила их оформления устанавливает Национальный Стандарт РФ ГОСТ Р 7.0.97-2016. «Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов».

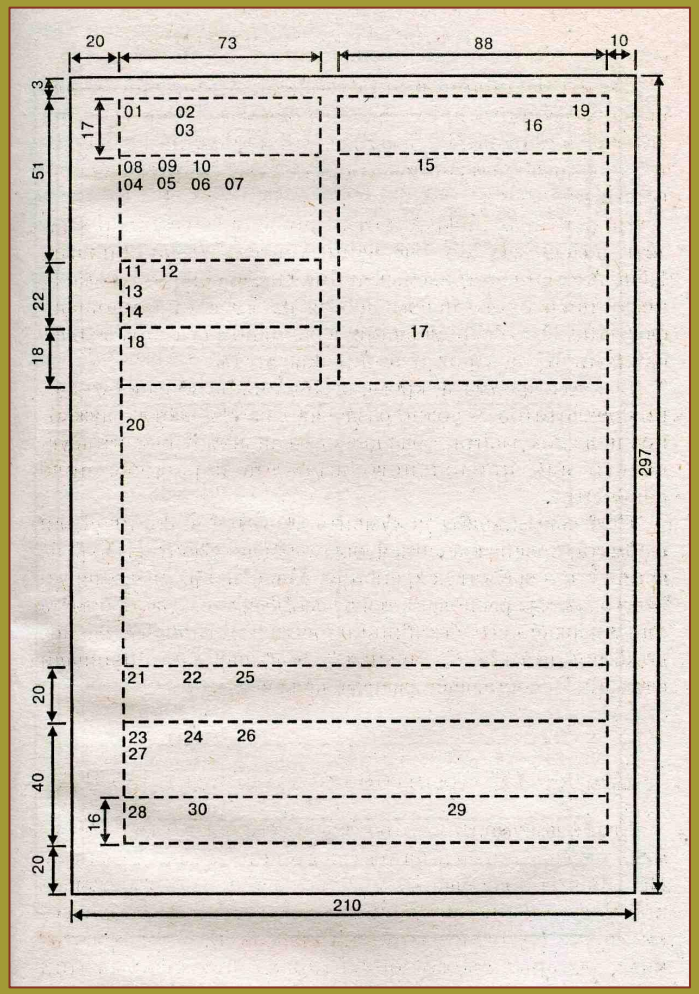
2.1.1. Состав и правила оформления реквизитов документов

При подготовке и оформлении ОРД используют следующие реквизиты:	
01 – Государственный герб Российской Федерации;	16 – гриф утверждения документа;
02 – герб субъекта Российской Федерации;	17 – резолюция;
03 – эмблема организации или товарный знак (знак обслуживания);	18 – заголовок к тексту;
04 – код организации;	19 – отметка о контроле;
05 – основной государственный регистрационный номер (ОГРН) юридического лица;	20 – текст документа;
06 – идентификационный номер налогоплательщика/код причины постановки на учет (ИНН/КПП);	21 – отметка о наличии приложения;
07– код формы документа;	22 – подпись;
08 – наименование организации;	23 – гриф согласования документа;
09– справочные данные об организации;	24 – визы согласования документа;
10 – наименование вида документа;	25 – оттиск печати;
11 – дата документа;	26 – отметка о заверении копии;
12 – регистрационный номер документа;	27 – отметка об исполнителе;
13 – ссылка на регистрационный номер и дату документа;	28 – отметка об исполнении документа и направлении его в дело;
14 – место составления или издания документа;	29 – отметка о поступлении документа в организацию;
15 – адресат;	30 – идентификатор электронной копии документа.

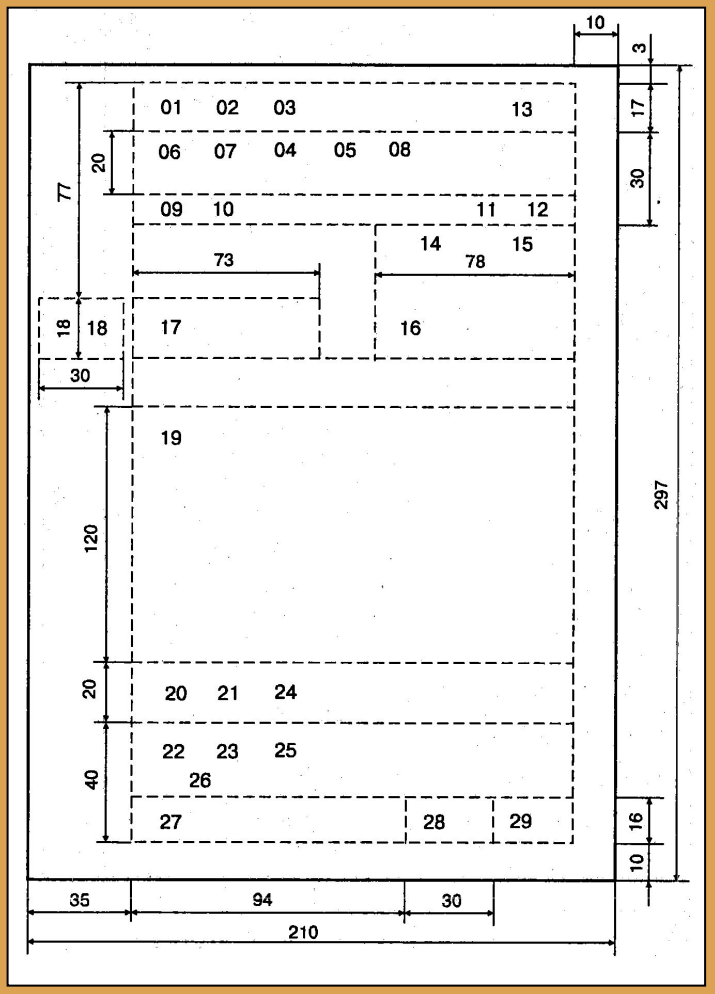
Установленные стандарты форматов бланков документов



Расположение реквизитов и границы зон на формате А4 углового бланка



Расположение реквизитов и границы зон на формате А4 продольного бланка



2.1.2. Правила машинописного и компьютерного оформления документов

Редактор - Word Windows (от 6.0 и выше)

Шрифт - Times New Roman Cyr

Размер - 12 (для оформления табличных материалов),

Размер -13

Размером - 14

Размером - 15

Межстрочный интервал – 1,5 (А4)

Межстрочный интервал – 1,0 (А5)

12345Первую строку каждого абзаца текста следует печатать, отступив на 5 знаков от границы левого поля.

Федеральное агентство по образованию
Государственное образовательное учреждение
высшего профессионального образования
«СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ГОУ ВПО «СибГТУ»)
Мира пр., д.82, Красноярск, 660049
Тел.: (3912) 66-03-88, факс: (3912) 63-61-17
E – mail: sibstu@sibstu.kts.ru,
http://www.sibstu.kts.ru
ОКПО 02067907,
ОГРН 1022402652359,
ИНН/КПП 2466003280/246601001
_____ № _____
На № _____ от _____

Угловой бланк письма организации

Федеральное агентство по образованию
Государственное образовательное учреждение высшего профессионального образования
«СИБИРСКИЙГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ГОУ ВПО «СибГТУ»)
Мира пр., д.82, Красноярск, 660049
Тел.: (3912) 66-03-88, факс: (3912) 63-61-17
E – mail: sibstu@sibstu.kts.ru, http://www.sibstu.kts.ru
ОКПО 02067907, ОГРН 1022402652359,
ИНН/КПП 2466003280/246601001
_____ № _____
На № _____ от _____

Продольный бланка письма организации

2.2. Структура защищаемых документопотоков, состав технологических этапов и операций

Как технологический процесс документооборот представляет собой схему (совокупность маршрутов) движения человекочитаемых (традиционных), машиночитаемых и электронных документов по установленным пунктам их учета, рассмотрения, исполнения и хранения для выполнения творческих, формально-логических и технических процедур и операций.

Документооборот как объект защиты представляет собой упорядоченную совокупность (сеть) каналов объективного, санкционированного распространения конфиденциальной документированной информации в процессе управленческой и производственной деятельности пользователей (потребителей) этой информации.

Наиболее часто встречающимися угрозами (опасностями) КД в документопотоках могут быть:

1. несанкционированный доступ постороннего лица к документам, делам и базам данных за счет его любопытства или обманных, провоцирующих действий, а также случайных или умышленных ошибок персонала фирмы;
2. утрата документа или его отдельных частей (листов, приложений, схем, копий, экземпляров, фотографий и др.), носителя чернового вари- анта документа или рабочих записей за счет кражи, утери, уничтожения;
3. утрата информацией конфиденциальности за счет ее разглашения персоналом или утечки по техническим каналам;
4. подмена документов, носителей и их отдельных частей с целью фальсификации, а также сокрытия факта утери, хищения;
5. случайное или умышленное уничтожение ценных документов и баз данных, несанкционированная модификация и искажение текста, реквизитов, фальсификация документов;
6. гибель документов в условиях экстремальных ситуаций.
7. Для электронных документов угрозы особенно реальны, так как факт кражи информации практически трудно обнаружить. В отношении КИ, обрабатываемой и хранящейся в компьютерах, условия возникновения угроз, классифицируются по степени риска следующим образом:
8. непреднамеренные ошибки пользователей, операторов, референтов, управляющих делами, работников службы КД, системных администраторов и других лиц, обслуживающих информационные системы;
9. кражи и подлоги информации;
10. стихийные ситуации внешней среды;
11. заражение вирусами.

Главным направлением защиты документированной информации от возможных опасностей являются формирование защищенного документооборота и использование в обработке и хранении документов специализированной технологической системы, обеспечивающей безопасность информации на любом типе носителя.

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:

1. ограничения доступа персонала к документам, делам и базам данных деловой, служебной или производственной необходимостью;
2. персональной ответственности должностных лиц за выдачу разрешения на доступ сотрудников к конфиденциальным сведениям и доку- ментам;
3. персональной ответственности каждого сотрудника за сохранность доверенного ему носителя и конфиденциальность информации;
4. жесткой регламентации порядка работы с документами, делами и базами данных для всех категорий персонала, в том числе первых руководителей.

Защищенность документопотоков достигается за счет:

1. одновременного использования режимных (разрешительных, ограничительных) мер и технологических приемов, входящих в систему обработки и хранения КД;
2. нанесения отличительной отметки (грифа) на чистый носитель КИ или документ, в том числе сопроводительный, что позволяет выделить их в общем потоке документов;
3. формирования самостоятельных, изолированных потоков КД и часто дополнительного их разбиения на подпотоки в соответствии с уровнем конфиденциальности перемещаемых документов;
4. использования автономной технологической системы обработки и хранения КД, не соприкасающейся с системой обработки открытых документов;
5. регламентации движения документов как внутри фирмы, так и между фирмами, т. е. с момента возникновения мысли о необходимости создания документа и до окончания работы с документом и передачи его в архив;

Входной документопоток включает в себя следующие стадии обработки КД:

1. прием, учет и первичная обработка поступивших пакетов, конвертов, незаконвертованных документов;
2. учет поступивших документов и формирование справочно-информационного банка данных по документам;
3. предварительное рассмотрение и распределение поступивших документов;
4. рассмотрение документов руководителями и передача документов на исполнение и технологические участки ПКД;
5. ознакомление с документами исполнителей, использование или исполнение документов.

Выходной и внутренний документопотоки включают в себя следующие стадии обработки КД:

1. исполнение документов (этапы: определение уровня грифа конфиденциальности предполагаемого документа, учет носителя будущего документа, составление текста, учет подготовленного документа, его изготовление и издание);
2. контроль исполнения документов;
3. обработка изданных документов (экспедиционная обработка документов и отправка их адресатам; передача изданных внутренних документов на исполнение);
4. систематизация исполненных документов в соответствии с номенклатурой дел, оформление, формирование и закрытие дел;
5. подготовка и передача дел в ведомственный архив (архив фирмы). В состав всех документопотоков включается также ряд дополнительных стадий обработки КД:
6. инвентарный учет документов, дел и носителей информации, не включаемых в номенклатуру дел;
7. проверка наличия документов, дел и носителей информации;
8. копирование и тиражирование документов;
9. уничтожение документов, дел и носителей информации.

Стадии, составляющие тот или иной документопоток, практически реализуются специализированной технологической системой обработки и хранения КД.

Следовательно, защита документированной информации в документопотоках обеспечивается комплексом разнообразных мер режимного, технологического, аналитического и контрольного характера.

Перемещение документов в процессе выполнения каждой стадии, этапа, процедуры обработки или исполнения сопровождается набором связанных учетных операций, закреплением документа за конкретным сотрудником и его персональной ответственностью за сохранность носителя КИ.

2.3. Технологические системы защиты и обработки конфиденциальных документов

Под технологической системой обработки и хранения КД понимается упорядоченный комплекс организационных и технологических процедур и операций, обеспечивающих служб и технических средств, предназначенных для практической реализации задач, стоящих перед функциональными элементами (стадиями) документопотока.

Технологическая система обработки и хранения КД решает следующие задачи:

1. обеспечения документированной информацией управленческих и производственных процессов;
2. обеспечение защиты носителей информации и самой информации от потенциальных и реальных угроз их безопасности.

К обработке КД предъявляются следующие серьезные требования:

1. централизация всех стадий, этапов, процедур и операций по обработке и хранению КД;
2. учет всех без исключения КД;
3. пооперационный учет технологических действий, производимых с традиционным (бумажным) или электронным носителем (в том числе чистым) и документом, учет каждого факта «жизненного цикла» документа;
4. обязательный контроль вторым работником службы КД правильности выполнения учетных операций;
5. учет и обеспечение сохранности не только документов, но и учетных форм;
6. ознакомление или работа с документом только на основании письменной санкции (разрешения) полномочного руководителя, письменного фиксирования всех обращений персонала к документу;
7. обязательная подпись руководителей, исполнителей и технического персонала при выполнении любых действий с документом в целях обеспечения персональной ответственности сотрудников фирмы за сохранность носителя и конфиденциальность информации;
8. строгий контроль выполнения персоналом введенных в фирме правил работы с КД, делами и базами данных, обязательными для всех категорий персонала;
9. систематические (периодические и разовые) проверки наличия документов у исполнителей, в делах, базах данных, на машинных носителях и т. д., ежедневный контроль сохранности, комплектности, целостности и местонахождения каждого КД;
10. коллегиальность процедуры уничтожения документов, дел и баз данных;
11. письменное санкционирование полномочным руководителем процедур копирования и размножения бумажных и электронных КД, контроль технологии выполнения этих процедур.

Технологические системы обработки и хранения КД

- Традиционные
- Автоматизированные
- Смешанные

Традиционная
(делопроизводственная) система основывается на ручных методах работы человека с документами и является универсальной.

Система характеризуется:

- ✔ низкой степенью оперативности доставки документов потребителям информации,
- ✔ невысокой эффективностью справочной, поисковой и контрольной работы по документам,
- ✔ потребностью в значительном количестве персонала, обслуживающего систему

Автоматизированная технология (как и традиционная, делопроизводственная) является обеспечивающей и обслуживает конкретные потребности персонала в КИ

Автоматизированная система, создаваемая ПКД или службе безопасности, должна, в принципе, обеспечивать:

1. сокращение значительного объема рутинной работы с документами и числа технических операций, выполняемых персоналом ПКД ручными методами;
2. реализацию возможности для персонала фирмы работать с электронными документами в режиме безбумажного документооборота;
3. достаточную гарантию сохранности и целостности информации, регулярного контроля и противодействия попыткам несанкционированного входа в банк данных;
4. аналитическую работу по определению степени защищенности информации и поиску возможных каналов ее утраты;
5. единство технологического процесса с режимными требованиями к защите информации (допуск, доступ, регламентация коллегиальности выполнения некоторых процедур, операций и т. п.);
6. персональную ответственность за сохранность конфиденциальных сведений в машинных массивах и на магнитных носителях вне ЭВМ;
7. возможность постоянного учета местонахождения традиционного или электронного документа и проверки его наличия и целостности в любое время;
8. предотвращение перехвата информации из ЭВМ по техническим каналам, наличие надежной охраны помещений, в которых находится вычислительная техника, охрана компьютеров и линии компьютерной связи;
9. исключение технологической связи единичного компьютера или локальной сети, предназначенных для обработки КД, с сетями, обеспечивающими работу с открытой информацией, исключение использования их линий связи, выходящих за пределы охраняемой зоны (здания, территории)

Автоматизированная технологическая система обработки и хранения КД по сравнению с аналогичными системами, оперирующими общедоступной информацией, имеет ряд принципиальных особенностей:

1. архитектурно компьютеры, обрабатывающие значительные объемы КИ, могут объединяться в локальную сеть как в рамках ПКД, так и с охватом руководителей и основных специалистов;
2. в некрупных фирмах конфиденциальная информация обрабатывается на уровне первого руководителя и его референта на единичном защищенном компьютере, не имеющем выхода в какую-либо локальную сеть;
3. обязательное наличие иерархической и утвержденной первым руководителем фирмы системы разграничения доступа к информации, хранящейся как в машинных массивах, так и на магнитных носителях вне ЭВМ;
4. закрепление за каждым пользователем строго определенного состава массивов электронной информации и магнитных носителей;
5. исключение возможности для пользователя покопаться в базе данных системы;
6. автоматизированное выполнение пользователями операции справочного и поискового обслуживания, составления и иногда изготовления документов, контроля исполнения документов, работы с электронными документами, факсами и электронными аналогами бумажных документов;
7. обязательный учет конфиденциальных электронных документов, находящихся на всех магнитных носителях и в машинных массивах, постоянная проверка службой КД реального наличия этих документов на носителях и в массивах, их целостности, комплектности и отсутствия несанкционированных копий;
8. необходимость исключения технической возможности копирования информации, содержащейся в компьютере (рабочей станции) пользователя, на другие магнитные носители и работы компьютера в комплекте с принтером (изъятие из ЭВМ дисководов и т. п.);
9. жесткое соблюдение персоналом правил работы с конфиденциальной электронной информацией, в частности правила, которое гласит, что все операции с информацией в компьютере должны быть письменно санкционированы полномочным должностным лицом, подотчетны службе КД и протоколироваться в машинном журнале; протоколы под- лежат регулярному контролю и анализу специалистами службы КД или службы безопасности;
10. изъятие КИ из базы данных компьютера (рабочей станции) по окончании работы с ней (например, в конце рабочего дня, при длительных перерывах в работе и т. п.) и перенос информации на дискеты, подлежащие сдаче в службу КД.
11. В настоящее время наиболее широко используется смешанная технологическая система обработки и хранения КД, совмещающая традиционную и автоматизированную технологии.