|  |  |  |
| --- | --- | --- |
| Удмуртский Государственный Университет | | |
| (наименование учебного заведения) | | |
| Кафедра Информационной безопасности в управлении | | |
| (наименование кафедры) | | |
| РЕФЕРАТ  по дисциплине  "Компьютерные информационные технологии  Документационного обеспечения управления"  на тему  "Защищенный документооборот -  проблемы и возможные решения" | | |
| Выполнила студентка  очной формы обучения  специальности ДиДОУ  4 курса 350800-41 группы | | Ю.А. Долганова |
| (инициалы и фамилия) |
| Руководитель проекта Старший преподаватель |  | Р.И. Исхаков |
| (ученая степень, звание) | | (инициалы и фамилия) |
| Город Ижевск  Год 2007 | | |

**Аннотация**

Данная работа посвящена раскрытию темы: «Защищенный документооборот – проблемы и возможные решения».

Реферат разделен на 2 главы, в которых последовательно рассмотрены теоретические и методические основы построения и организации защищенного документооборота.

В первом подразделе работы дана краткая теоретическая справа о документообороте, указаны цель и определение документооборота. Так же указаны виды угроз, которые могут возникнуть в документопотоках организации для конфиденциальных документов.

Во втором подразделе указаны основные группы проблем, возникающие при обеспечении информационной безопасности электронного документооборота.

Работа службы ДОУ тесно связана с деятельностью службы ИТ. Но в ходе их сотрудничества часто возникает непонимание в сфере построения защищенного документооборота, чему посвящен третий подраздел I главы.

Во втором разделе поочередно описаны организация документооборота и конфиденциального делопроизводства, даются ссылки на действующие нормативные акты и методические пособия по данной теме.

Как известно, организация конфиденциального документооборота должна строиться на основе определенных принципов, которые подробно расписаны в третьем подразделе II главы.

С уничтожением документов может увеличиться риск утечки конфиденциальной информации. Чтобы избежать этого – следует уничтожать не только сам документ, но и физический носитель информации (дискеты, диски и т.п.), для чего требуется специальные технические средства. Данной теме посвящен четвертый пункт II главы.

Далее – предлагается проект разрешительной системы доступа к конфиденциальным документам, перечисляются пункты, за счет которых достигается защищенность документопотоков от несанкционированного доступа.

Данные пункты поочередно раскрываются в процессе раскрытия выбранной мною темы: «Защищенный документооборот – проблемы и возможные решения».

# Содержание

[Введение 5](#_Toc164233992)

[1. Теоретические основы построения документооборота 7](#_Toc164233993)

[1.1. Краткая теоретическая справка о документообороте 7](#_Toc164233994)

[1.2. Информационная безопасность электронного документооборота 10](#_Toc164233995)

[1.3. Взаимоотношение ДОУ и ИТ 12](#_Toc164233996)

[2. Методические основы построения и организации защищенного документооборота 14](#_Toc164233997)

[2.1. Организация документооборота 14](#_Toc164233998)

[2.2. Организация конфиденциального делопроизводства 15](#_Toc164233999)

[2.3. Принципы защиты конфиденциального документооборота 18](#_Toc164234000)

[2.4. Уничтожение документов с истекшими сроками хранения 19](#_Toc164234001)

[2.5. Разрешительная система доступа к конфиденциальным документам 20](#_Toc164234002)

[Заключение 22](#_Toc164234003)

[Список использованной литературы 23](#_Toc164234004)

# Введение

На сегодняшний день одной из важнейших проблем, стоящих как в государственных, так и в негосударственных структурах, является проблема построения защищенного документооборота.

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.

Проблема защиты информационных ресурсов организации гораздо более сложная и многоплановая чем может показаться на первый взгляд, и для её успешного решения необходимо использовать не только силы и средства, имеющиеся в распоряжении службы информационных технологий, но и возможности и опыт, накопленный другими службами организации. С моей точки зрения на каждом предприятии должны защищаться все информационные ресурсы организации, в этой работе должны участвовать все сотрудники организации, и для достижения требуемого уровня безопасности должны активно применяться кадровая политика, разнообразные организационные меры, обучение и переподготовка персонала и т.п.

Сейчас в организациях вопросами управления и защиты информации занимается целый ряд служб. Служба информационных технологий (ИТ) традиционно обеспечивает работоспособность, защиту электронных систем от несанкционированного доступа, в то время как служба Документационного обеспечения управления (ДОУ) - работает в основном с бумажными документами. Правда, в последние 10 лет, большинство крупных предприятий в г. Ижевске пытаются перейти на безбумажный документооборот, что получается пока далеко не у всех предприятий. Кроме того, есть ещё юридический отдел, отдел информационной безопасности. Различная подчинённость и статус этих служб, незнакомство с методами работы друг друга, отсутствие единой терминологии становятся серьёзной помехой в решении поставленных перед ними задач.

**Целью** написания данной работы является раскрытие темы «Защищенный документооборот – проблемы и возможные решения». В этой работе будет рассмотрена организация документооборота не с точки зрения службы ИТ, а с точки зрения ДОУ.

Данная цель будет раскрыта в рамках конкретных **задач**:

* будут раскрыты теоретические основы построения защищенного документооборота;
* и методические основы и построения и организации защищенного документооборота.

# 1. Теоретические основы построения документооборота

## 1.1. Краткая теоретическая справка о документообороте

Документооборот предприятия определяется как «движение документов с момента их получения или создания до завершения исполнения, отправки или сдачи в дело».

**Целью документооборота** является обеспечение управленческой деятельности, процесса принятия решений ценной, полезной, своевременной, полной и достоверной информацией. Движение документированной информации (на бумажных, магнитных или иных носителях) по линиям связи объективно сопровождает управленческую деятельность. Принципы и направления движения традиционных и электронных документов в аппарате управления едины при любых системах обработки и хранения документированной информации. Меняются методы работы с документами, но технологическая взаимосвязь документооборота с процессом управления сохраняется. Это предпосылка создает объективную возможность для научного решения документоведческих и архивоведческих проблем безбумажного документооборота.

Все документы являются информационными материалами (информацией), но далеко не все информационные материалы имеют статус документа. Основной признак документа состоит в том что, содержание, обстоятельства создания и форма представления информационного материала фиксируются в определённый момент времени, и далее хранятся в неизменном виде. Кроме того, документ либо фиксирует какие-либо факты и события, либо служит основанием для принятия деловых решений и совершения действий.

С учетом всего сказанного можно дать **определение конфиденциального документооборота** как движение конфиденциальных документов с момента их учета до отправления, подшивки в дело или перевода на учет выделенного хранения поступивших и изданных документов и отправления, уничтожения или передачи на архивное хранение документов выделенного хранения.

Вместе с тем, важной отличительной чертой и особенностью конфиденциального документооборота является необходимость защиты документов от несанкционированного доступа к ним с целью предотвращения утечки конфиденциальной информации.

Стандарт ISO/IEC 17799 определяет информационную безопасность как обеспечение конфиденциальности, целостности и наличия информации. Что касается защиты электронных документов и электронного документооборота, - на данный момент данную функцию выполняет служба ИТ.

**Виды угроз конфиденциальных документов в документопотоках организации можно разделить на несколько групп:**

1. Несанкционированный доступ постороннего лица к документам, делам, базам данных за счет его любопытства или обманных, провоцирующих действий, а так же случайных или умышленных ошибок персонала фирмы;
2. Утрата документа или его отдельных частей (листов, приложений, схем, копий, экземпляров, фотографий и др.), носителя чернового варианта документа или рабочих записей за счет кражи, утери, уничтожения;
3. Утрата информацией конфиденциальности за счет ее разглашения персоналом или утечки по техническим каналам, считывания данных в чужих массивах, использования остаточной информации на копировальной ленте, бумаге, дисках и дискетах, ошибочных действий персонала;
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.

Для **электронных документов** угрозы особенно реальны, так как факт кражи информации практически трудно обнаружить. В отношении конфиденциальной информации, обрабатываемой и хранящейся в компьютерах, условия возникновения угроз, по мнению ряда специалистов, классифицируется по степени риска следующим образом:

* + Непреднамеренные ошибки пользователей, операторов, референтов, управляющих делами, системных администраторов и других лиц, обслуживающих информационные системы;
  + Кражи и подлоги информации;
  + Стихийные ситуации внешней среды;
  + Заражение вирусами.

В соответствии с характером указанных выше угроз формируется задачи обеспечения защиты информации в документопотоках, направленные на предотвращение или ослабление этих угроз.

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

Таким образом, **безопасность – это не только защита от преступных посягательств, но и обеспечение сохранности (особенно электронных) документов и информации, а также меры по защите важнейших документов, и обеспечению непрерывности и/или восстановлению деятельности в случае катастроф.**

## 1.2. Информационная безопасность электронного документооборота

С XX века во многих странах мира стали активно внедряться различные системы электронного документооборота. Защита электронного документооборота от несанкционированного доступа стала одной из главных проблем, находящихся на сегодняшний день в сфере бизнеса. В связи с этим можно выделить **три группы проблем**, которые возникают при обеспечении информационной безопасности электронного документооборота:

* **Трудности, связанные с недостаточной поддержкой государством внедрения систем электронного документооборота (СЭД)**. Пока государство и суды не признают электронные документы, бизнес может использовать СЭД только для поддержки оперативной деятельности. Хотя с недавнего времени на некоторых предприятиях стала активно внедряться электронно-цифровая подпись (ЭЦП). Но она применяется далеко не на всех предприятиях и государством более признаются «бумажные» документы», т.е. данная отрасль является неразвитой.
* **Отсутствие нормативной базы, необходимой для полноценного использования электронных документов.** Так, не установлен порядок признания юридической силы электронных документов государственными органами и судами; отсутствует официально признаваемая методика работы с электронными документами, обеспечивающая признание их юридической силы; отсутствуют методики экспертизы ценности электронных документов, передачи их на архивное хранение, уничтожения электронных документов, работы с «грифованными» электронными документами, и т.д.

**Перечисленные проблемы напрямую связаны с информационной безопасностью.** Пока что электронные документы – вроде и не документы вовсе, и во многих организациях с ними поступают, как хотят. Часто отсутствует даже элементарный учёт имеющихся в организации программных средств и баз данных, а в результате электронные документы и информация либо утрачиваются, либо их становится невозможно ни найти, ни использовать. Уничтожение увольняющимися сотрудниками «своих» электронных богатств – самое обычное явление, с которым невозможно бороться.

* **Сохранение аутентичности и целостности электронных документов.** На сегодняшний день электронные документы мало признаются судами – отсюда следует вывод: если сегодня не начать архивировать электронные документы в строгом соответствии с известными международными стандартами, то завтра, когда электронные документы будут признаны на деле, организация не сможет доказать подлинность своих документов. Для компаний, ведущих международную деятельность, это уже «горящая» проблема, поскольку, к примеру, в большинстве развитых стран сообщения электронной почты признаются деловыми документами и могут быть предъявлены в качестве доказательства в суде.

**Проблема обеспечения аутентичности электронных документов особенно обостряется, если их нужно хранить долго – более 5-7 лет.** В этом случае, вследствие устаревания компьютерных систем и/или форматов данных, может потребоваться перенос документов в другую компьютерную систему и/или преобразование в новые форматы. Более того, каждый шаг переноса документов и преобразование из в новые форматы должен быть тщательно задокументирован для того, чтобы аутентичность документов не могла быть подвергнута сомнению.

Но даже при обычном сканировании документов для помещения их в электронный архив требуется не только документировать все действия и обеспечить техническую защиту полученных образов документов, но и избегать операций, которые могут поставить аутентичность документов под сомнение.

## 1.3. Взаимоотношение ДОУ и ИТ

При внедрении систем электронного документооборота на уровне отдельной организации особую остроту приобретает проблема взаимоотношений и взаимопонимания между службой ИТ с одной стороны, и службой ДОУ, юридическим отделом и деловыми подразделениями – с другой.

Прежде всего, это проблема «делового статуса». ИТ-специалисты стоят на более высокой ступени в иерархии организации, имеют большую зарплату, пользуются гораздо большим влиянием на руководство. В коммерческих структурах денег на развитие современных технологий не жалеют, в то время как отделы ДОУ получают средства на свое развитие по остаточному принципу. Кроме того, специалисты ДОУ жалуются на то, что служба ИТ определяет требования к управлению документами, не консультируется с ДОУ при выборе и закупке систем электронного документооборота.

Именно продолжающееся внедрение информационных технологий в процесс документооборота, в сочетании с усиливающимся давлением со стороны законодательства и контролирующих органов, потихоньку приводит к изменению положения ДОУ в лучшую сторону – поскольку ряд знаний и навыков, обычных для сотрудников нашей службы и остро необходимых сейчас в электронном документообороте, не распространены среди специалистов ИТ.

К ним относятся:

1. Понимание жизненного цикла документа, который может включать такие стадии, как создание, временное хранение в соответствии с требованиями законодательства и контролирующих инстанций, экспертизу ценности, постоянное хранение или уничтожение в установленном порядке;
2. Понимание того, что вся информация организации должна управляться по единым правилам;
3. Привычка веси строгий учёт документов, их выдачи и возврата;
4. В отличие от большинства программистов, сотрудники ДОУ вынуждены продумывать свою работу как минимум на пять лет вперёд (столько времени, по закону, должны храниться документы бухгалтерского учёта). Они понимают, что нужно не просто сохранить соответствующие электронные документы, но сохранить их так, чтобы их целостность и аутентичность могла быть доказана.

Именно специалисты службы ДОУ лучше других видят проблемы, возникающие при внедрении. Особенное беспокойство вызвало то, что сотрудники ИТ и деловых подразделений плохо понимают роль электронного документооборота в обеспечении соответствия деятельности организации законодательству и нормативным требованиям.

**Для успешного внедрения электронных систем и их надёжной защиты необходимо тесное сотрудничество специалистов ИТ, ДОУ и других заинтересованных сторон: деловых подразделений, юридической службы, службы информационной безопасности.** В перспективе, одним из разумных решений может быть переход службы ДОУ в подчинение ИТ, и создание единого подразделения, управляющего всеми информационными ресурсами в организации. Подобные единые структуры уже существуют как за рубежом, так и в ряде организаций нашей страны.

# 2. Методические основы построения и организации защищенного документооборота

## 2.1. Организация документооборота

Установление порядка движения документов или управление документацией организации заключается в создании условий, обеспечивающих хранение необходимой документной информации, ее быстрый поиск и снабжение ею потребителей в установленные сроки и с наименьшими затратами. Она включает:

* организацию документооборота;
* создание информационно-поисковых систем по документам;
* контроль их исполнения;
* подготовку документов к передаче на архивное хранение.

По определению "Движение документов с момента их получения или создания до завершения исполнения, отправки адресату или сдачи на хранение" образует документооборот. Соответственно масштабам движения документов можно выделить документооборот конкретного должностного лица, структурного подразделения, организации, отрасли управления, государства в целом.

Действующие нормативные акты и методические документы, в том числе и «Государственная система документационного обеспечения управления. Основные положения. Общие требования к документам и службам документационного обеспечения» (ГСДОУ), исходя из прагматических соображений, рассматривают в качестве объекта регулирования только документооборот организации в целом и соответственно потоки входящих, внутренних и исходящих документов.

ГСДОУ требует закрепления порядка движения документов внутри организаций в схемах, разрабатываемых службой делопроизводства и утверждаемых руководством организаций. В подобные схемы должны быть включены все, в том числе и компьютерные пункты обработки документной информации и, если они поддаются нормированию, сроки прохождения и обработки документов. Самостоятельные схемы разрабатываются для различных категорий документов: входящих, исходящих, внутренних, приказов по личному составу и по основной деятельности и т.д. В эти схемы включаются, как правило, этапы создания документов от момента написания черновика. В случае утверждения схем движения документов руководством организации они приобретают нормативную силу.

Документооборот, или порядок движения документов в организации, можно разделить на следующие **этапы**:

1. Экспедиционная обработка документов, поступающих в организацию.

2. Предварительное рассмотрение документов службой документационного обеспечения.

3. Рациональное движение документов внутри организации.

4. Обработка исполненных и отправляемых документов.

## 2.2. Организация конфиденциального делопроизводства

Правильная организация конфиденциального делопроизводства в фирме является составной частью комплексного обеспечения безопасности информации и имеет важное значение в достижении цели ее защиты. Как известно, специалисты, занимающиеся в области информационной безопасности утверждают, что порядка 80% конфиденциальной информации находится в документах делопроизводства. Поэтому вопросы конфиденциального документооборота в фирме несомненно играют важную роль в достижении ею экономических успехов. В данной статье даны некоторые рекомендации, позволяющие упорядочить работу в фирме с конфиденциальными документами.

Всю информацию в фирме (организации) можно разделить на две большие группы:

* открытую;
* с ограниченным доступом.

В свою очередь **информация с ограниченным доступом** может быть:

* государственной тайной;
* конфиденциальной информацией.

А, следовательно, и **документы**, содержащие ту или иную информацию подразделяются на **секретные и конфиденциальные**. Причем, секретные документы могут быть **с грифом "Секретно", "Совершенно секретно", "Особой важности".** Конфиденциальные документы соответственно **с грифами "Коммерческая тайна"** и т.д.

В настоящее время видов конфиденциальной информации (а, следовательно, и возможных грифованных документов) насчитывается более 30. Что в целом не создает благоприятной атмосферы в смысле обеспечения их безопасности. По этой причине количество видов конфиденциальной информации в перспективе, надо полагать, уменьшится. Каждый вид конфиденциальных документов имеет реквизиты.

По своей природе конфиденциальные документы бывают:

* нормативно-методические;
* руководящие;
* распорядительные;
* информационно-справочные;
* организационные;
* финансово-бухгалтерские;
* кадровые (по личному составу).

Конфиденциальные документы должны обрабатываться в конфиденциальном делопроизводстве фирмы, либо в общем делопроизводстве, специально назначенным должностным лицом, ответственным за конфиденциальные документы. Конфиденциальные документы должны храниться в отдельном помещении в запираемых и опечатываемых шкафах. Допускается хранение конфиденциальных документов в общем делопроизводстве. Но обязательно они должны находиться отдельно от других дел делопроизводства.

В зависимости от назначения **конфиденциальные документы подразделяются на:**

* входящие;
* исходящие;
* внутренние.

Прием входящих конфиденциальных документов осуществляется сотрудником конфиденциального делопроизводства.

При этом проверяется:

* количество листов;
* количество экземпляров;
* наличие приложений (если они указаны в сопроводительном письме).

В случае отсутствия в пакете (конверте) некоторых перечисленных документов - составляется акт в 2-х экземплярах. Один экземпляр акта отправляется в адрес отправителя.

Регистрация документов производится в электронной базе, в журналах регистрации, либо на карточках.

На каждом зарегистрированном документе должен проставляться штамп, в котором указывается:

* наименование;
* регистрационный номер;
* дата поступления.

После регистрации документы передаются руководству органиизации для принятия решения. Руководитель после рассмотрения документа определяет исполнителя и дает указания по исполнению документа. Эти указания оформляются на самом документе в виде резолюции.

С резолюцией руководителя конфиденциальный документ передается исполнителю под расписку в журнале регистрации входящих конфиденциальных документов.

По завершении работы над документом на нем проставляется отметка о его исполнении и направлении в дело. После чего документ сотрудником конфиденциального делопроизводства подшивается в дело.

Все дела с конфиденциальными документами и журналы их учета вносятся в номенклатуру дел организации.

По окончании каждого года руководителем организации создается комиссия, которая должна:

* проверить наличие конфиденциальных документов;
* определить конфиденциальные документы для архивного хранения;
* определить конфиденциальные документы, подлежащие уничтожению.

В случае утери конфиденциального документа руководителем организации создается комиссия, которая проводит расследование по факту утраты данного документа. По результатам работы комиссии руководителем организации принимается решение о привлечении к ответственности лиц виновных в утрате конфиденциального документа.

## 2.3. Принципы защиты конфиденциального документооборота

Организация конфиденциального документооборота должна строиться на основе следующих **принципов**:

* Разрешительной системы доступа к конфиденциальным документам;
* Обеспечения пользователей всеми необходимыми им в силу служебных обязанностей конфиденциальными документами, но только теми, которые действительно необходимы для выполнения конкретных видов работы;
* Исключения несанкционированного доступа к конфиденциальным документам;
* Целенаправленного регулирования процессов движения конфиденциальных документов;
* Исключения инстанций прохождения конфиденциальных документов и действий с ними, не обусловленных характером и порядком исполнения документов;
* Фиксированной передачи конфиденциальных документов;
* Обеспечения своевременного и качественного исполнения конфиденциальных документов;
* Персональной и обязательной ответственности за выдачу неправомерных разрешений и ознакомление с конфиденциальными документами и на их отправление.

Как и многие другие задачи, проблема защиты конфиденциального документооборота решается только в том случае, когда служба ДОУ, отвечающая главным образом за «бумажную» работу, и служба информационных технологий, контролирующая сегодня электронные документы и материалы, объединяются в единое целое и действуют совместно.

## 2.4. Уничтожение документов с истекшими сроками хранения

Возможность вполне законно уничтожить документы по истечении срока хранения - чрезвычайно важный элемент всей работы по обеспечению информационной безопасности. Это возможность уменьшить риск утечки конфиденциальной информации.

В бумажном делопроизводстве, уничтожение документов и предшествующий этап экспертизы их ценности считаются наиболее сложными видами работ, требующими как высокой профессиональной квалификации, так и умения взаимодействовать практически со всем коллективом организации. С электронными документами нужно решать все те же проблемы, что и с бумажными, плюс ещё несколько – порой очень трудно разыскать и уничтожить все имеющиеся копии электронного, к тому же, как выяснилось на практике, **гарантированное уничтожение электронных документов требует физического уничтожения носителей этих документов, для чего требуются специальные технические средства.**

## 2.5. Разрешительная система доступа к конфиденциальным документам

Разрешительная система доступа к конфиденциальным документам представляет собой совокупность установленных руководством предприятия нормативных положений, обеспечивающих обоснованный и правомерный доступ пользователей к необходимому им для выполнения служебных обязанностей объему конфиденциальных документов. Системой должно быть определено, кто из руководителей предприятия и структурных подразделений, кому из пользователей и с какими категориями конфиденциальных документов может давать разрешение на ознакомление (работу), а также порядок оформления таких разрешений в зависимости от вида учета или категорий документов. При этом право давать разрешение на ознакомление и право работать с конфиденциальными документами может быть предоставлено только лицам, имеющим допуск к коммерческой тайне.

При установлении разрешительной системы доступа к конфиденциальным документам необходимо учитывать следующие требования:

* соответствующий руководитель может давать разрешение на ознакомление с конфиденциальными документами, входящими в сферу его деятельности. Только подчиненным лицам и только по служебной необходимости;
* разрешение на ознакомление оформляется письменно;
* при необходимости ознакомления пользователя только с частью конфиденциального документа в разрешении на ознакомление должны быть указаны разделы, пункты или страницы, с которыми можно знакомить пользователя.

Разрешительная система должна предусматривать и порядок доступа к конфиденциальным документам лиц, не работающих на данном предприятии (при выполнении совместных работ и др.). За разглашение или неправомерное использование содержащихся в документах конфиденциальной информации сотрудники, получившие доступ к конфиденциальным документам несут перед обладателем этих документов гражданско-правовую ответственность.

**Защищенность документопотоков достигается за счет:**

* одновременного использования режимных (разрешительных, ограниченных) 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;
* формирования самостоятельных, изолированных потоков конфиденциальных документов и часто дополнительного их разбиения на подпотоки в соответствии с уровнем конфиденциальности перемещаемых документов;
* использования автономной технологической системы обработки и хранения конфиденциальных документов, не соприкасающихся с системой обработки открытых документов;
* 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;
* организации самостоятельного подразделения конфиденциальной документации или аналогичного подразделения, входящего (или не входящего) в состав службы безопасности или аналитической службы;
* перемещения документов между руководителями, исполнителями и иным персоналом только через службу конфиденциального делопроизводства.

# Заключение

Я постаралась учесть как можно больше аспектов по построению защищенного документооборота и представить ряд требований, которые позволяли построить систему безопасного обращения документов в любой структуре как государственной, так и коммерческой. К сожалению, в нашей стране проблеме построения защищенного документооборота уделяется не так много внимания, какое стоило бы уделить. На каждом предприятии в идеале должен учитываться человеческий фактор, ужесточены рамки наказания за разглашения секретной информации, должны быть поощрения за правильное ведение делопроизводственных операций.

Нужно учитывать, что безопасность – это не только защита от преступных посягательств, но и обеспечение сохранности (особенно электронных) документов и информации, а также меры по защите важнейших документов и обеспечению непрерывности и/или восстановлению деятельности в случае катастроф.

Гарантированное уничтожение электронных документов требует не только физического уничтожения бумажного документа, а также физического уничтожения носителей этих документов, для чего требуются специальные технические средства.

Я считаю, что обеспечение информационной безопасности требует решения многочисленных проблем, и их, безусловно, не под силу в одиночку решить ни службе ИТ, ни службе ДОУ, ни какой-либо другой. Только координированная работа всех служб под единым руководством, при понимании и поддержке, как со стороны высшего руководства, так и персонала организации может привести к успеху. Особенно, важна интеграция ИТ и ДОУ в единую службу управления документами и информацией, при этом сотрудники ДОУ должны понимать и активно использовать современные технологии в своей работе, а сотрудники ИТ – лучше относиться к потребностям деловых подразделений организации и к вопросам, связанным с соблюдением законодательных и нормативных требований к документообороту.

# Список использованной литературы

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне».
3. Федеральный закон 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи».
4. ГОСТ Р 6.30-2003. Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов.
5. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.
6. Алексенцев А.И. Конфиденциальное делопроизводство. – М.: ЗАО «Бизнес-школа «Интел-Синтез». – 2001. – 90-93 с.
7. «Единый регламент осуществления делопроизводственных операций на предприятии ОАО «Удмуртнефть»» (по стандартам «Росснефть»). - 2007.
8. Кузнецова Т.В. Делопроизводство (документационное обеспечение управления). 4-е изд. испр. и допол. М: Изд-во ЮНИТИ, 2003 – 322 с.
9. Организация работы с документами: Учебник / Под ред. проф. Кудряева В.А. – 2-е изд., перераб. и допол. – М.: ИНФРА-М, 2001. – 592 с.
10. Сабынин В.Н. Организация конфиденциального делопроизводства - начало обеспечения безопасности информации в фирме // Информост-радиоэлектроника и телекоммуникации. - 2001. - № 4. – с. 17.
11. Степанов Е.А. Информационная безопасность и защита информации: Учебное пособие // Е.А. Степанов, И.К. Корнеев - М.: ИНФРА-М – 2001 – 107-111с.
12. Храмцовская Н.А. Информационная безопасность доку­менто­обо­ро­та с точки зрения специалиста ДОУ (http://eos.ru/eos/134718).
13. Храмцовская Н.А. Общие проблемы внедрения систем электронного документооборота в отечественном бизнесе (http://www.gdm.ru/meropr/ 181004/book/hramtsovskaya1.shtml).
14. Сайт Домарева В.В. «Безопасность информационных технологий» (http://www.security.ukrnet.net).