Южно-Российский региональный учебно-научный центр по проблемам информационной безопасности ЮФУ, в г.Таганроге.

«Защищенный документооборот»

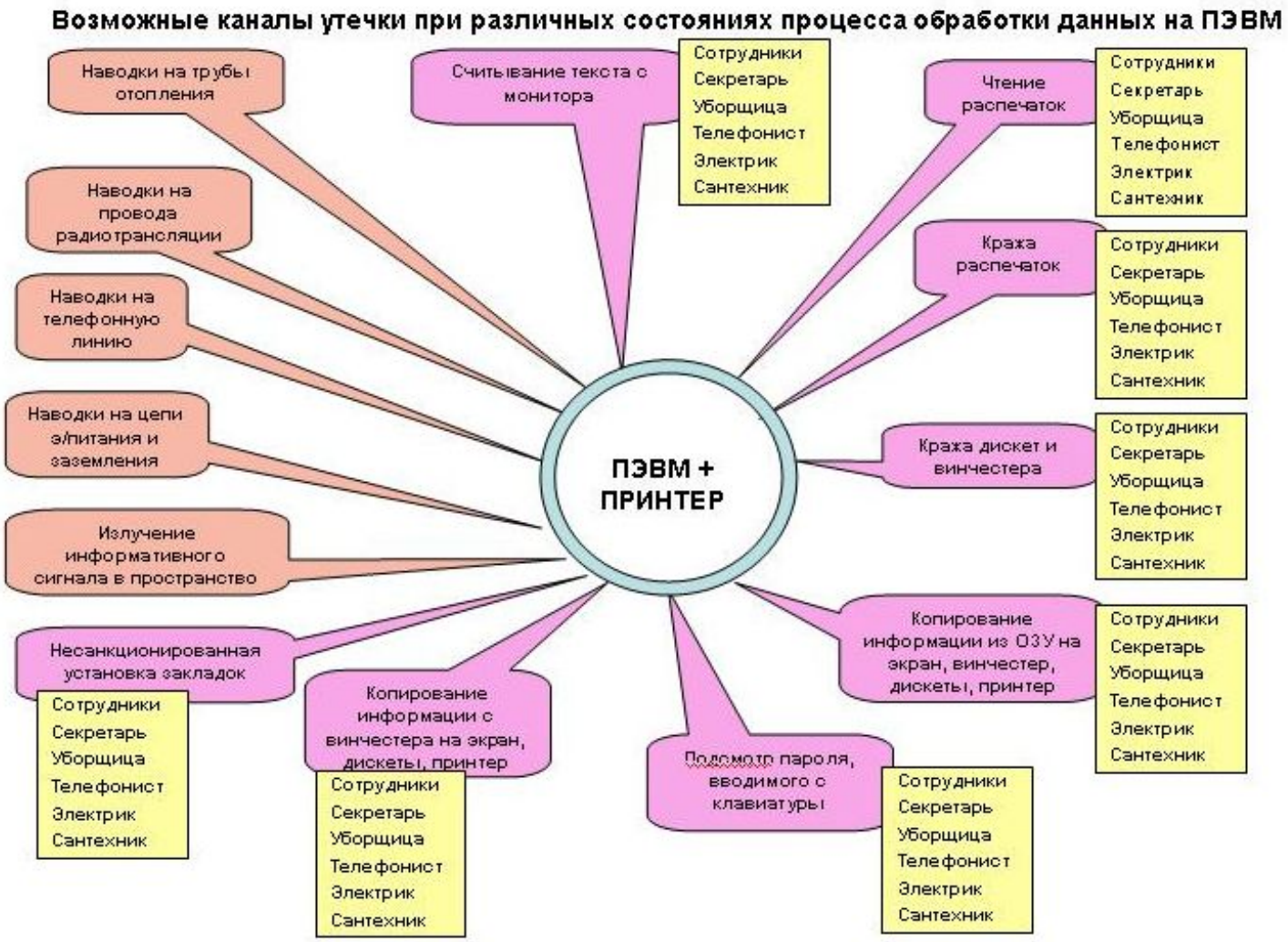
Защита информации

1. Защита системы (или нескольких систем, комплекса систем), в которой обрабатываются данные.
2. Защита непосредственно данных (документов и информации) внутри системы (систем).

Что включает в себя Защита данных:

- Обеспечение доступа к данным, непредставляющего угрозы для них (защита от несанкционированного доступа), и разграничение прав пользователя на работу с этими данными.
- Обеспечение сохранности данных.
- Защиту от некорректных действий пользователей с данными.
- Обеспечение конфиденциальности данных - шифрование.
- Обеспечение целостности данных (защита от повреждения и уничтожения информации, искажения информации как ненамеренного в случае ошибок и сбоев, так и злоумышленного) и подтверждение авторства - электронная подпись.

Возможные каналы утечки данных



Основные регламентирующие документы

1. **ФЗ РФ № 19-ФЗ от 02.02.2006 г.** «О правовой охране программ для ЭВМ и баз данных» .

2. **ФЗ РФ № 1-ФЗ от 10.01.2002 г.** «Об электронной цифровой подписи».

3. **ФЗ РФ № 98-ФЗ от 29.07.2004 г.** «О коммерческой тайне».

4. **ФЗ РФ № 125-ФЗ от 22.10.2004 г.** «Об архивном деле в Российской Федерации».

5. **ФЗ РФ № 149-ФЗ от 27.07.2006 г.** «Об информации, информационных технологиях и о защите информации».

6. **Указ Президента РФ от 14.01.19922 г. № 20** «О защите государственных секретов Российской Федерации».

7. **Указ Президента РФ от 23.09.2005 г. № 188** « Об утверждении перечня сведений конфиденциального характера».

8. **Указ Президента РФ от 12.05.2004 г. № 611** «О мерах по обеспечению информационной безопасности РФ в сфере международного информационного обмена».

9. **Указ Президента РФ от 30.11.1995 г.** «Об утверждении перечня сведений, отнесённых к государственной тайне».

10. **Постановление Правительства РФ от 3.11.1994 г. № 1233** «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

Основные регламентирующие документы

11. **Приказ Министерства культуры и массовых коммуникаций РФ от 8.11.2005 г.**

«О типовой инструкции по делопроизводству в федеральных органах исполнительной власти».

12. **Приказ ФСБ РФ от 9.02.2005 г.** «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005).

13. Приказ ФСБ РФ, ФСТЭК РФ от 31.08.2010 г. № 416/489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования».

14. Постановление Правительства РФ от 17.11.2007 г. «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

15. **Инструкция Главгосэкспертизы РФ** «О порядке обращения с документированной служебной информацией ограниченного распространения в организациях, учреждениях, предприятиях и т.д.».

16. Приказ **Министерства образования и науки РФ от 10.08.2012 г. № 606** «О внесении изменений в приказ Министерства образования и науки РФ от 30.12.2010 г. № 2233 «Об утверждении инструкции о порядке обращения со служебной информацией ограниченного распространения в Министерстве образования и науки РФ».

Основные регламентирующие документы

ГОСТ Р 51141-98

ДЕЛОПРОИЗВОДСТВО И АРХИВНОЕ ДЕЛО . Термины и определения

ГОСТ Р 50922-2006

Защита информации. Основные термины и определения

ГОСТ Р ИСО 9001-2008

Системы менеджмента качества. Требования

ГОСТ Р ИСО 15489-1-2007

Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования

ГОСТ Р 1.12-2004

Стандартизация в Российской Федерации. Термины и определения

ГОСТ Р 1.10-2004

Стандартизация в Российской Федерации. Правила стандартизации и рекомендации по стандартизации. Порядок разработки, утверждения, изменения, пересмотра и отмены

Основные регламентирующие документы

ГОСТ Р 6.30-2003

Унифицированная система организационно-распорядительной документации. Требования к оформлению документов.

ГОСТ 6.10.4-84

Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники

ГОСТ Р 1.4-2004

Стандартизация в Российской Федерации. Стандарты организаций. Общие положения

ГОСТ Р 1.5-2004

Стандартизация в Российской Федерации. Стандарты национальные Российской Федерации. Правила построения, изложения, оформления и обозначения

ГОСТ Р 1.0-2004

Стандартизация в Российской Федерации
Основные положения

ГОСТ Р 34.10-2001

Информационная технология. Криптографическая защита информации . Процессы формирования и проверки электронной цифровой подписи

Термины и определения

Защита информации - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.
Собственником информации могут быть: государство, юридическое лицо, группа физических лиц, отельное физическое лицо.

Организация защиты информации - содержание и порядок действий, направленных на обеспечение защиты информации.

Защищенный документооборот (документопоток) - контролируемое движение конфиденциальной документированной информации по регламентированным пунктам приема, обработки, рассмотрения, исполнения, использования и хранения в условиях организационного и технологического обеспечения безопасности, как носителя информации, так и самой информации.

Термины и определения

Документы, содержащие информацию, составляющие коммерческую (служебную) тайну или имеющими гриф **«Для служебного пользования»** принято называть **конфиденциальными документами**, а процессы изготовления таких документов и организацию работы с ними - **конфиденциальным делопроизводством**.

К документированной служебной информации, ограниченного распространения, относится несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью.

Необходимость присвоения документам грифа **«Для служебного пользования»** («ДСП») определяется исполнителем и должностным лицом, подписывающим или утверждающим документ, в соответствии с «Перечнем видов служебной информации», которую необходимо относить к разряду ограниченного распространения (утверждается руководителем организации).

Конфиденциальность информации - обязательное требование для выполнения лицом, получившим доступ к определенной информации, не передавать такую информацию третьим лицам без согласия ее обладателя.

Термины и определения

Коммерческая тайна - это информация, включающая формулу, состав, комбинацию, программу, приспособление, метод, технику или процесс, которая: имеет самостоятельную экономическую стоимость (используемую или потенциальную) благодаря тому, что не является общеизвестной или доступной людям, которые могут использовать ее в коммерческих целях.

Под коммерческой тайной предприятия понимаются не являющиеся государственными секретами сведения, связанные с производством, технологической информацией, управлением, финансами и другой деятельностью предприятия, разглашение (передача, утечка) которых может нанести ущерб его интересам.

Коммерческая тайна - вид тайны, включающий информацию, устанавливаемую и защищаемую ее обладателем в любой сфере его коммерческой деятельности, доступ к которой ограничивается в интересах обладателя информации.

Носитель информации - физическое лицо или материальный объект, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов.

ПЕРЕЧЕНЬ СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА

(в ред. Указа Президента РФ от 23.09.2005 N 1111)

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 г. N 119-ФЗ "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства" и другими нормативными правовыми актами Российской Федерации.
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.

К документированной служебной информации ограниченного распространения не могут быть отнесены:

- акты законодательства, устанавливающие правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;
- сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов;
- описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также его адрес; порядок рассмотрения и разрешения заявлений, а также обращений граждан и юридических лиц;
- решения по заявлениям и обращениям граждан и юридических лиц, рассмотренным в установленном порядке;
- документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах, необходимые для реализации прав, свобод и обязанностей граждан.

Основные угрозы для конфиденциальных документов

1. Несанкционированный доступ постороннего лица к документам, делам и базам данных за счет его любопытства или обманных действий, а также случайных или умышленных ошибок персонала учреждения, фирмы.

2. Утрата документа или его отдельных частей, носителя чернового варианта документа или рабочих записей в случае кражи, утери, уничтожения.

3. Утрата информацией конфиденциальности при ее разглашении персоналом или утечке по техническим каналам считывания данных, передаваемых по незащищённым каналам связи, использовании остаточной информации на бумаге, дисках, ошибочные действия персонала.

4. Подмена документов, носителей и их отдельных частей с целью фальсификации и 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.

Основные принципы работы с защищенными документами

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

ЗАЩИЩЕННЫЙ ДОКУМЕНТООБОРОТ ОСНОВЫВАЕТСЯ НА РЯДЕ СЛЕДУЮЩИХ 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 документам;

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 т.ч. первых руководителей.

Защищенность документопотоков достигается за счет:

1. Одновременного использования режимных (разрешительных, ограничительных) мер и технологических приемов, входящих в систему обработки и хранения конфиденциальных документов;
2. Нанесения отличительной отметки (грифа) на чистый носитель конфиденциальной информации или документ, в т.ч. сопроводительный, что позволяет выделить их в общем потоке документов;
3. Формирования самостоятельных изолированных потоков конфиденциальных документов. Дополнительное их разбиение на подпотоки, в соответствии с уровнем конфиденциальности перемещаемых документов;
4. Использования автономной технологической системы обработки и хранения конфиденциальных документов, не соприкасающейся с системой обработки открытых документов;
5. Регламентации движения документов как внутри учреждения, так и между учреждениями, т.е. с момента возникновения мысли о необходимости создания документа и до окончания работы с документом и передачи его в архив;
6. Организации самостоятельного подразделения (службы) конфиденциальной документации;
7. Перемещения документов между руководителями, исполнителями и иным персоналом только через специальное подразделение (службу), которое занимается защищённым документооборотом.

Обработка конфиденциальных документов

Входной документопоток включает следующие стадии обработки конфиденциальных документов:

1. Прием, учет и первичную обработку поступивших 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 в службу контроля документов;
5. Ознакомление с документами исполнителей, использование или исполнение документов.

Обработка конфиденциальных документов

Выходной и внутренний документопотоки включают следующие стадии обработки конфиденциальных документов:

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 за исполнением документов;
3. Обработка изданных документов (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 учреждения.

Обработка конфиденциальных документов

В состав всех документопотоков также входит ряд дополнительных стадий обработки конфиденциальных документов:

1. Инвентарный учет документов, дел и носителей информации, не входящих в номенклатуру дел;
2. Проверка наличия документов, дел и носителей информации;
3. Копирование и тиражирование документов;
4. Уничтожение документов, дел и носителей информации.

Порядок обращения с документами содержащими сведения ограниченного распространения

Руководители структурных подразделений учреждений, организаций, предприятий и т.д. принявшие решение об отнесении документированной служебной информации к разряду ограниченного распространения, несут персональную ответственность за обоснованность принятого решения и соблюдение ограничений, а также за обеспечение защиты носителей информации ограниченного распространения и использование средств оргтехники при подготовки этих документов.

Документированная служебная информация, ограниченного распространения, без указаний руководителя организации или его заместителей не подлежит разглашению (распространению).

За разглашение документированной служебной информации ограниченного распространения, а также нарушение порядка обращения с документами, содержащими такую информацию, сотрудник организации может быть привлечен к дисциплинарной или иной предусмотренной законодательством ответственности.

Сотрудники организаций, имеющие отношение к работе с документами, делами и зданиями «Для служебного пользования» , должны быть в обязательном порядке ознакомлены с инструкцией, устанавливающей порядок работы с документированной информации ограниченного распространения в организации.

Работа с документами ДСП

Для работы с ДСП документами необходимо:

1. Сформировать перечень сведений конфиденциального характера (утверждается руководителем организации);
2. Документально оформить список сотрудников, допущенных к сведениям конфиденциального характера;
3. Назначить сотрудника или подразделение, которое будет заниматься ДСП делопроизводством;
4. Разработать инструкцию по ДСП делопроизводству;
5. Определить помещение, места хранения документов ;
6. Аттестовать ПЭВМ по требованиям безопасности;
7. Определить сотрудников, допущенных к обработке информации на АРМ;
8. Разработать документы для работы на АРМ.

Этапы исполнения документа на АРМ

1. Исполнение документа на черновике
2. Заполнение технического задания
3. Исполнение документа на АРМ
4. Регистрация документа в журнале учёта
5. Ознакомление с документом (отправка документа адресату)
6. Уничтожение черновиков документа

Создание документов на АРМ

Создание документов, относящихся к служебной информации ограниченного распространения осуществляется на специально выделенном автоматизированном рабочем месте, с закрытым доступом в общую информационную систему, определенном решением руководителя. Создание иных документов на нем запрещается. Учет созданных документов со служебной информацией ограниченного распространения осуществляется в журнале учета.

За АРМ закрепляются работники из числа лиц, допущенных к служебной информации ограниченного распространения. Данные работники несут ответственность за правильное использование АРМ, осуществляют допуск к нему и контроль за правильным оформлением разрабатываемых документов.

АРМ обозначается табличкой размером 297 х 120 мм следующего содержания: "Место для разработки документов с пометкой "ДСП". Табличка устанавливается на видном месте.

Создание документов на АРМ

Разрешается хранение на АРМ созданных проектов документов с пометкой «ДСП» в электронном виде. На обороте последнего листа каждого экземпляра документа исполнителем указываются количество отпечатанных экземпляров, кому они направляются, фамилия исполнителя, рабочий телефон и дата печатания документа. Отпечатанные и подписанные документы вместе с черновиками и вариантами передаются для регистрации работнику, осуществляющему их учет. Черновики и варианты документа с пометкой "ДСП" на бумажном носителе уничтожаются его исполнителем с отражением факта уничтожения в журнале учета документов со служебной информацией ограниченного распространения (их черновиков), подлежащих уничтожению. Уничтожение документов осуществляется с использованием бумагорезательной машины.

Размножаются (тиражируются) только с письменного разрешения должностного лица, уполномоченного относить служебную информацию к разряду ограниченного распространения.

Пример оформления документа

Для служебного пользования
экз. № ____

Текст документа

Пример оформления документа

Отп. 2 экз.
Экз. № 1
Исп. …….
10 листов
20.11.2012 г.

Порядок обращения с документами

Хранятся в надежно закрываемых на замок шкафах (ящиках, хранилищах), опечатываемых печатью установленного образца. Ответственность за правильное оборудование мест для хранения документов возлагается на руководителя. Запрещается хранение у работников документов в местах, не отвечающих этим требованиям. В случае отсутствия у работника, получившего документ, оборудованного места для его хранения, работа с документом осуществляется только в течение рабочего времени. До окончания рабочего времени полученный работником документ сдается на хранение.

Уничтожение дел, документов с пометкой "Для служебного пользования", утративших свое практическое значение и не имеющих исторической ценности, производится по акту.

При смене работника, ответственного за учет документов с пометкой "Для служебного пользования", составляется акт приема, передачи документов и материалов к ним.

Порядок приема и учета документов

1. Осуществляется подразделениями (или сотрудниками) которым поручен учёт этих документов.
2. Проверяется количество листов и экземпляров, наличие приложений.
3. Регистрации подлежат все входящие и исходящие документы.
4. Учитываются отдельно от несекретной информации. При незначительном объеме таких документов разрешается вести их учет совместно с другими несекретными документами. При регистрации указанных документов к регистрационному индексу документа добавляется пометка «ДСП».
5. Учёт документов ДСП ведётся на карточках или в журналах.
6. На каждом зарегистрированном документе проставляется штамп, в котором указываются наименование организации, регистрационный номер и дата его поступления.
7. Дополнительно размноженные экземпляры документа (издания) учитываются за номером этого документа.