МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования

«Юго-Западный государственный университет»

(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ

Проректор по учебной работе

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ О.Г. Локтионова

«\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2017 г.

**ЗАЩИТА И ОБРАБОТКА КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ**

Методические указания по выполнению самостоятельных работ

для студентов направления подготовки бакалавриата 10.03.01«Информационная безопасность»

Курск 2017

УДК 621. (076.1)

Составитель: О.А. Демченко

Рецензент

Кандидат технических наук, доцент кафедры «Информационная безопасность» И.В. Калуцкий

**Защита и обработка конфиденциальных документов** [Текст]: методические указания по выполнению самостоятельных работ/ Юго-Зап. гос. ун-т; сост.: О.А. Демченко. – Курск, 2017. – 33 с.: ил. 0. – Библиогр.: с. 36.

Содержат сведения по вопросам самостоятельных работ по защите и обработка конфиденциальных документов. Указывается порядок выполнения самостоятельных работ, правила оформления отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов направления подготовки бакалавриата 10.03.01 «Защита и обработка конфиденциальных документов».

Текст печатается в авторской редакции

Подписано в печать . Формат 60х84 1/16. Усл.печ. л. 2,09. Уч.-изд. л. 1,89. Тираж 100 экз. Заказ. Бесплатно.

Юго-Западный государственный университет.

305040, г.Курск, ул. 50 лет Октября, 94.

**Самостоятельная работа №1** – Основные понятия и определения в области защиты и обработки конфиденциальных документов

Целью изучения дисциплины «Защита и обработка конфиденциальных документов» является формирование у студентов базовых знаний о технологиях защищенного документооборота в условиях применения разнообразных носителей документальной информации (бумажных, магнитных и др)

Задачи курса – получение знаний о:

* месте конфиденциального документооборота в любых структурах государственной и негосударственной сфер;
* документальном обеспечении всех видов конфиденциальной деятельности;
* принципах защиты, содержащейся в конфиденциальных документах информации;
* методах и технологии конфиденциального документооборота;
* научных, методических и прикладных аспектах организации технологии защиты и обработки конфиденциальных документов

Конфиденциальная информация — это сведения, независимо от формы их предоставления, которые не могут быть переданы лицом, получившим доступ к данным сведениям, третьим лицам без согласия их правообладателя.

Сведения конфиденциального характера:

1. персональные данные;
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. № 119 – ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» и другими нормативными правовыми актами Российской Федерации;
3. служебная тайн;
4. врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений;
5. коммерческая тайна;
6. сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Перечень обязательных мер по охране конфиденциальности информации, которые должны приниматься ее обладателем:

1. определение перечня информации, составляющей коммерческую тайну;
2. ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
3. учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;
4. регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско – правовых договоров;
5. нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа «Коммерческая тайна» с указанием обладателя этой информации (для юридических лиц — полное наименование и место нахождения).

**Контрольные вопросы:**

1. Что является целью изучения дисциплины?
2. Каковы задачи данного курса?
3. Что такое конфиденциальная информация?
4. Какую информацию можно отнести к конфиденциальной?
5. Какие меры можно предпринять для защиты конфиденциальной информации?

**Самостоятельная работа №2** – Определение документа, классификация документов. Реквизиты документа. Типы реквизитов. Копия документа. Дубликат документа.

Документ (от лат. documentum — образец, свидетельство, доказательство)

Всякая важная деловая бумага, также диплом, свидетельство (Толковый словарь живого великорусского языка Владимира Даля)

Письменный акт, служащий свидетельством какого-либо решения, сделки или действия; деловая бумага, относящаяся к канцелярскому производству (Малый энциклопедический словарь Брокгауза и Ефрона)

Материальный объект с информацией, закрепленной созданным человеком способом для ее передачи во времени и пространстве. (Большой юридический словарь)

Деловая бумага, юридически подтверждающая определенные права ее обладателей, фиксирующая, удостоверяющая определенные факты, события; Информация, сведения, данные, зафиксированные на материальном носителе (бумаге, фотопленке, магнитном диске), имеющие официальный характер и подлежащие использованию или последующей обработке и передаче адресату.(Современный экономический словарь)

Зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать (ГОСТ Р 51141-98 «Делопроизводство и архивное дело»)

Классификация документов.

**По содержанию:**

* научно-технические (монографии, книги, патенты);
* правовые (постановления, указы, договоры и др.);
* управленческие (приказы, директивы).

**По времени создания:**

* первичные (указы, монографии);
* вторичные (рефераты, методические рекомендации).

**По способу изготовления/представления**:

* рукописные документы (служебная записка, объяснительная);
* машинописные документы (приказ, отчет);
* документы на машинном носителе (файлы);
* фонодокументы (звукозапись);
* кино- (видео) документы.

**По виду зафиксированной информации:**

* письменные (с использованием знаков письма);
* изобразительные (рисунок, фотография);
* идиографические (карты, ноты, схемы);
* аудиовизуальные (звук, изображение).

**По способу чтения:**

* человекочитаемые;
* машиночитаемые

**По месту издания:**

* внутренние;
* внешние;

**По направлению отправки/получения:**

* входящие;
* исходящие.

Копия документа. Дубликат документа

**Официальный документ -** документ, созданный юридическим или физическим лицом, оформленный и удостоверенный в установленном порядке

**Копия документа** - документ, полностью воспроизводящий информацию подлинного документа и все его внешние признаки или часть их, не имеющий юридической силы…»

**Заверенная копия документа** - копия документа, на которую в соответствии с установленным порядком проставляют необходимые реквизиты, придающие ей юридическую силу…»

При заверении соответствия копии документа подлиннику ниже реквизита **"Подпись"** проставляют заверительную надпись: "Верно"; должность лица, заверившего копию; личную подпись; расшифровку подписи (инициалы, фамилию); дату заверения.

Допускается копию документа заверять **печатью**, определяемой по усмотрению организации.

При рассылке документов, имеющих нормативный правовой характер (постановления, приказы, распоряжения и т.д.), размноженные экземпляры рассылаемых документов следует заверять **печатью организации** или **печатью структурного подразделения**, например: печатью с наименованием службы ДОУ организации (канцелярии, общего отдела и т.п.).

**Контрольные вопросы:**

* 1. Что такое документ?
  2. Какие виды документов вам известны?
  3. Какой документ является оффициальным?
  4. Что такое копия документа?

**Самостоятельная работа №3** – Документационное обеспечение управления. Принципы организации документооборота на предприятии.

Документационное обеспечение управления

**Документационное обеспечение управления (ДОУ)** или **делопроизводство** **–** это отрасль деятельности, обеспечивающая документирование и организацию работы с официальными документами.

ГОСТ Р 51141-98 «Делопроизводство и архивное дело. Термины и определения»

Термин **"документационное обеспечение управления"** подчеркивает информационно-технологическую составляющую в современной организации делопроизводства и его лучше употреблять, когда речь идет о компьютерных технологиях работы с документами. Термин **"делопроизводство"** преимущественно используется при описании организационной стороны и традиционных приемов работы с документами.

**Две составные части документационного обеспечения управления (ДОУ) или делопроизводства**

* документирование деятельности (создание документов);
* организация работы с официальными документами:
  + учет (регистрация);
  + хранение документов;
  + использование документов в текущей деятельности организации

Документация — совокупность документов, посвященных какому-либо вопросу.

Система документации — совокупность документов, взаимосвязанных по признакам происхождения, назначения, вида, сферы деятельности, единых требований к их оформлению.

**Документооборот организации** – это движение документов в организации с момента их создания или получения до завершения исполнения или отправления. В целях рациональной организации документооборота все документы распределяются на документопотоки:

- поступающие (входящие) документы;

- отправляемые (исходящие) документы;

- внутренние документы.

Характеристикой документооборота является его **объем,** под которым понимается **количество документов,** **поступивших** в организацию и **созданных** ею за определенный период. Данный показатель является важным, он должен использоваться в качестве критерия при выборе организационной формы делопроизводства (традиционная, автоматизированная), а также влиять на структуру службы делопроизводства и ее штатный состав.

**Принципы организации документооборота**

В управлении широко используются электронные средства создания и обработки документов, поэтому **документооборот рассматривается как составная часть информационного обеспечения управления** и включает в себя движение информационных потоков организации – их получение, обработку, переработку, использование

Какая бы технология обработки документов ни использовалась, **организация документооборота должна основываться на определенных принципах, или правилах, обеспечивающих оперативное прохождение документов по наиболее короткому пути с минимальными затратами времени**. К таким принципам организации документооборота относятся следующие

* **централизация операций по приему, первичной обработке и отправке документов (это означает, что все документы, поступающие в организацию всеми способами доставки (по почте, факсу, электронной почте и др.) и отправляемые из организации, обрабатываются в службе ДОУ);**
* **максимальное сокращение числа инстанций прохождения и исключение возвратных движений документа, не обусловленных деловой необходимостью (возвратным считается такое движение документа, при котором он поступает в ту инстанцию, в которой уже проходил обработку);**
* **маршрутизация отдельных видов документов** (разработка схем прохождения документов);
* **однократность регистрации документов** (документы, поступающие в организацию и создаваемые в организации, регистрируются один раз: входящие – при поступлении, внутренние и исходящие – при создании; регистрация документов может осуществляться в службе ДОУ учреждения или в структурном подразделении);
* **организация предварительного рассмотрения документов** (распределение документов, поступивших в организацию, на документы, направляемые на резолюцию руководителю, его заместителям и передаваемые на исполнение непосредственно в подразделения; предварительное рассмотрение проводит специалист службы ДОУ (секретарь-референт или помощник руководителя);
* **вынесение конкретных резолюций,** по возможности точно определяющих исполнителя, поручение, срок исполнения;
* **исключение необоснованных согласований**, организация параллельного согласования документов одновременно несколькими работниками (копирование проекта документа или передача его по электронной почте одновременно всем заинтересованным лицам);
* **снижение уровня** подписания документов.

Жизненный цикл документа.Некоторые особенности документооборота

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.

**Контрольные вопросы:**

1. Что означает термин «делопроизводство»?
2. Каковы основные принципы организации документооборота?
3. Перечислите этапы жизненного цикла дркументооборота.

**Самостоятельная работа №4** – Понятия, задачи и функции конфиденциального делопроизводства.

Методология формирования требований к системе защищенного документооборота

Конкретные требования к защите документооборота, обусловленные спецификой автоматизированной обработки информации, определяются совокупностью следующих факторов:

* характером обрабатываемой информации;
* объемом обрабатываемой информации;
* продолжительностью пребывания информации в АСОД;
* структурой АСОД; видом защищаемой информации;
* технологией обработки информации;
* организацией информационно-вычислительного процесса в АСОД;
* этапом жизненного цикла АСОД.

Классификация требований к системе защищенного документооборота

**Требования, определяемые характером информации**

при обработке общедоступной информации никаких специальных мер защите от несанкционированного доступа не требуется;

требования к защите конфиденциальной информации определяет пользователь, устанавливающий статус конфиденциальности;

требования к защите грифованной информации определяются следующим образом:

при обработке информации с грифом «Для служебного пользования» к ней должен быть обеспечен свободный доступ пользователям учреждения-владельца этой информации; доступ же пользователей, не включенных в общий список, должен осуществляться по разовым санкциям, выдаваемым пользователями, включенными в список

Требования, определяемые структурой АСОД

В аппаратуре и линиях связи:

1. защищаемая информация должна находиться только в течение сеанса; в ЗУ аппаратуры связи могут храниться только служебные части передаваемых сообщений;

2. линии связи, по которым защищаемая информация передается в явном виде, должны находиться под непрерывным контролем во все время передачи информации;

3. перед началом каждого сеанса передачи защищаемой информации должна осуществляться проверка адреса выдачи данных;

4. при передаче большого объема защищаемой информации проверка адреса передачи должна также периодически производиться в процессе передачи (через заданный промежуток времени или после передачи заданного числа знаков сообщения);

5. при наличии в составе аппаратуры связи процессоров и ЗУ должна вестись регистрация данных о всех сеансах передачи защищаемой информации;

6. должны быть предусмотрены возможности аварийного уничтожения информации, находящейся в аппаратуре связи.

В центральном вычислителе:

1. защищаемая информация в ОЗУ может находиться только во время сеансов решения соответствующих задач, в ВЗУ - минимальное время, определяемое технологией функционирования автоматизируемых процессов;

2. и 3.— аналогично соответствующим пунктам требований к защите УГУВВ;

4. при обработке защищаемой информации должно осуществляться установление подлинности всех участвующих в обработке устройств и пользователей и ведение протоколов их работы;

5. всякое обращение к защищаемой информации должно проверяться на санкционированность;

6. при обмене защищаемой информации, осуществляемой с использованием линий связи, должна осуществляться проверка адреса корреспондента;

7. должны быть предусмотрены возможности аварийного уничтожения

всей информации, находящейся в центральном вычислителе, и подачи команды на аварийное уничтожение информации в сопряженных устройствах.

В ВЗУ:

1. сменные носители информации должны находиться на устройствах управления в течение минимального времени, определяемого технологией автоматизированной обработки информации;

2. устройства управления ВЗУ, на которых установлены, носили с защищаемой информацией, должны иметь замки, предупреждающие несанкционированное изъятие или замену носителя;

3. должны быть предусмотрены возможности автономного аварийного уничтожения информации на носителях, находящихся на устройствах ВЗУ.

В хранилище носителей:

1. все носители, содержащие защищаемую информацию, должны иметь четкую и однозначную маркировку, которая, однако, не должна раскрывать содержания записанной на них информации;

2. носители, содержащие защищаемую информацию, должны храниться таким образом, чтобы исключались возможности несанкционированного доступа к ним;

3. при выдаче и приемке носителей должна осуществляться проверка личности получающего (сдающего) и его санкции на получение (сдачу) этих носителей;

4. должны быть предусмотрены возможности аварийного уничтожения информации на носителях, находящихся в хранилищах.

В устройствах подготовки данных:

1. защищаемая информация должна находиться только в течение времени ее подготовки;

2. устройства подготовки должны быть размещены так, чтобы исключались возможности просмотра обрабатываемой информации со стороны;

3. в специальных регистрационных журналах должны фиксироваться время обработки информации, исполнители, идентификаторы использованных носителей и возможно другие необходимые данные;

4. распределение работ между операторами должно быть таким, чтобы минимизировать осведомленность их о содержании обрабатываемой информации;

5. должны быть предусмотрены возможности аварийного уничтожения информации, находящейся в подразделениях подготовки данных.

Требования к защите информации, обуславливаемые   
территориальной распределенностью АСОД

в компактных АСОД (размещенных в одном помещении) достаточно организовать и обеспечить требуемый уровень защиты в пределах того помещения, в котором размещены элементы АСОД;

в слабораспределенных АСОД (размещенных в нескольких помещениях, но на одной и той же территории) дополнительно к предыдущему должна быть обеспечена требуемая защита информации в линиях связи, с помощью которых сопрягаются элемен­ты АСОД, расположенные в различных помещениях, для чего должны быть или постоянный контроль за этими линиями связи, или исключена передача по ним защищаемой информации в явном виде;

в сильнораспределенных АСОД (размещенных на нескольких территориях) дополнительно *к предыдущему должна быть обеспечена требуемая защита информации в линиях связи большой протяженности, что может быть достигнуто предупреждением передачи по ним защищаемой информации в открытом виде.*

**Контрольные вопросы:**

1. Исходя из каких факторов определяются конкретные требования к защите документооборота?
2. Классификация требований к системе защищенного документооборота
3. Перечислите Требования, определяемые характером информации.
4. Требования, определяемые структурой АСОД.
5. Требования к защите информации, обуславливаемые территориальной распределенностью АСОД.
6. Требования, обусловливаемые видом защищаемой информации
7. Специфические требования.

**Самостоятельная работа №5** – Организация конфиденциального документооборота на предприятии.

**Учет документов с грифом «Конфиденциальная информация»**

Все документы с грифом «Конфиденциальная информация», изданные или поступившие на предприятие, подлежат учету в подразделении по ведению делопроизводства документов с грифом «Конфиденциальная информация».

Учет документов с грифом «Конфиденциальная информация» осуществляется отдельно от учета секретных и несекретных, а также с грифом «Для служебного пользования» документов.

Виды учета:

- учет входящих документов;

- учет исходящих (подготовленных) документов;

- инвентарный учет;

- номенклатура дел, журналов, карточек.

Прием и регистрация документов с грифом «Конфиденциальная информация» осуществляется подразделением по ведению делопроизводства документов с грифом «Конфиденциальная информация». Однократная регистрация распространяется и на документы с грифом «Конфиденциальная информация».

Если на предприятии вся получаемая корреспонденция поступает в экспедицию, а также при получении корреспонденции в нерабочее время дежурным по предприятию, пакеты с грифом «Конфиденциальная информация» не вскрываются и передаются в подразделение по ведению делопроизводства документов с грифом «Конфиденциальная информация».

Ошибочно поступившие документы с грифом «Конфиденциальная информация» возвращаются отправителю.

В случае отсутствия (недостачи) в пакетах документов (экземпляров, листов, приложений) с грифом «Конфиденциальная информация» составляется акт (приложение № 1) в двух экземплярах, один из которых высылается отправителю.

Регистрация поступивших документов с грифом «Конфиденциальная информация» производится на карточках (приложение № 2) или в журналах, которые должны иметь аналогичные грифы.

Картотеки или журналы учета входящих документов с грифом «Конфиденциальная информация» учитываются в номенклатуре. Листы журналов нумеруются, прошиваются и опечатываются.

На первом листе зарегистрированного входящего документа с грифом «Конфиденциальная информация» проставляется штамп, в котором указывается наименование предприятия, входящий номер документа, дата регистрации, количество листов основного документа и приложений.

Печатание документов с грифом «Конфиденциальная информация» производится в машбюро подразделения по ведению делопроизводства документов с грифом «Конфиденциальная информация». По решению руководителя предприятия печатание может быть разрешено в рабочих помещениях исполнителей документов при условии исключения получения охраняемой информации посторонними лицами.

На последнем листе каждого экземпляра отпечатанного документа необходимо проставить количество отпечатанных экземпляров, фамилию исполнителя документа, фамилию машинистки или лица, печатавшего документ и дату.

Отпечатанный документ, а также материалы, подготовленные в рукописном или графическом исполнении, регистрируются в подразделении по ведению делопроизводства документов с грифом «Конфиденциальная информация» на карточках (приложение № 3) или в журналах, имеющих соответствующие графы.

Картотеки или журналы учета подготовленных документов с грифом «Конфиденциальная информация» учитываются в номенклатуре. Листы журналов нумеруются, прошиваются и опечатываются.

Учетные номера проставляются на первом листе каждого экземпляра документа, а также на последнем листе перед отметкой о количестве отпечатанных экземпляров.

Все черновики, а также варианты и испорченные при печатании листы должны быть сданы в подразделение по ведению делопроизводства документов с грифом «Конфиденциальная информация» для уничтожения.

Инвентарному учету подлежат разработанные на предприятии и присланные из других предприятий научно-технические, чертежно-конструкторские и другие документы, не подлежащие подшивке в дела. Присланные документы берутся на инвентарный учет после их регистрации по входящему учету и рассмотрения соответствующими должностными лицами.

На инвентарный учет не берутся технические и другие документы, подшиваемые в дела, а также документы, присланные на согласование и во временное пользование.

В зависимости от специфики предприятия, количества документов инвентарный учет может вестись раздельно по наименованиям и видам документов, а также по видам производства.

Инвентарный учет ведется по карточкам (приложение № 4) или журналам, имеющим графы, аналогичные графам карточки. Листы журналов нумеруются, прошиваются и опечатываются. Картотеки или журналы учитываются в номенклатуре.

На инвентарный учет берутся подготовленные подлинники технических документов. Копии учитываются за номером оригинала. Если документ изготавливается машинописным способом и черновик уничтожается сразу после изготовления подлинника, то на инвентарный учет берется подлинник, а в карточке (журнале) учета делается отметка об уничтожении черновика.

На документах, взятых на инвентарный учет, проставляется штамп с указанием инвентарного номера и даты регистрации.

Штамп с инвентарным номером проставляется:

на сброшюрованных документах - в верхнем левом углу обложки и титульного (первого) листа документа;

на документах, хранящихся россыпью - в верхнем левом углу каждого листа;

на графических документах - над основной надписью.

Дела, журналы, картотеки с грифом «Конфиденциальная информация» учитываются по общей номенклатуре дел предприятия.

В графе 1 номенклатуры под индексом, присвоенным данному делу, журналу, картотеке, проставляется гриф «Конфиденциальная информация». После графы «Заголовок дела» вводится графа «Фамилии исполнителей, которым предоставлено право пользования делом».

Для подразделения по ведению делопроизводства документов с грифом «Конфиденциальная информация» делается выписка из номенклатуры, в которую вносятся все дела, журналы и картотеки с грифом «Конфиденциальная информация».

При составлении номенклатуры дел, включающей дела с грифом «Конфиденциальная информация», кроме учета требований общего делопроизводства о порядке комплектования дел в соответствии с различными признаками классификации необходимо предусмотреть круг лиц, имеющих право пользоваться делом, не допуская необоснованного его расширения, но и не затрудняя решение производственных вопросов.

Документы с грифом «Конфиденциальная информация» подшиваются в дела в соответствии с выпиской из номенклатуры после их исполнения. Все дела с грифом «Конфиденциальная информация» независимо от сроков их хранения должны иметь внутреннюю опись, которая выполняет функцию учета документов внутри каждого дела.

Листы дела нумеруются, после закрытия дела прошиваются и опечатываются. Заверительный лист подписывается сотрудником подразделения по ведению делопроизводства документов с грифом «Конфиденциальная информация».

**Контрольные вопросы:**

1. Как ведется учет документов с грифом «Конфиденциальная информация»?
2. Какие виды учета вам известны?
3. Как производится регистрация документов с грифом «конфиденциальная информация»?

**Самостоятельная работа №6** – Перечень сведений конфиденциального характера. Жизненный цикл конфиденциального документа.

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).
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.

**Контрольные вопросы:**

1. Какие сведения можно отнести к конфиденциальным?
2. Какого вида информация содержится в конфеденциальных документах?

**Самостоятельная работа №7** – Структура системы получения разрешения на доступ к конфиденциальной информации предприятия (разрешительная система доступа).

**Назначение разрешительной системы**

**Разрешительная система** - это совокупность правил, регулирующих порядок доступа работников предприятия и других лиц к сведениям (работам, документам изделиям), являющимся конфиденциальной информацией.

**Целями** введения Разрешительной системы на предприятии являются:

- исключение несанкционированного или необоснованного ознакомления со сведениями, являющимися конфиденциальной информацией;

- своевременное обеспечение требующейся грифованной информацией исполнителей работ и документов.

**Схема выдачи разрешений на доступ сотрудников предприятия к сведениям, составляющим конфиденциальную информацию**

Схема выдачи разрешений на доступ сотрудников предприятия к охраняемой информации является ключевым элементом, определяющим эффективность Разрешительной системы в целом.

Поэтому, при разработке «Схемы...» необходимо в полной мере учитывать структуру предприятия, сложившуюся систему управления, производственные связи внутри предприятия, распределение обязанностей между заместителями руководителя предприятия и т. д. Следует также иметь в виду, что чрезмерные ограничения в выдаче разрешений на доступ к охраняемой информации неизбежно приведут к снижению оперативности в решении производственных вопросов, в то время как излишняя либерализация создаст условия для утечки сведений, составляющих конфиденциальную информацию предприятия.

Выдача разрешения на доступ сотрудников предприятия к сведениям, составляющим конфиденциальную информацию, будет полной и удобной в работе, если проработать и изложить ее в 2-х аспектах:

* выдача разрешений в зависимости от категорий документов;
* выдача разрешений в зависимости от занимаемой должности.

Схема выдачи разрешений в зависимости от категории документов.

Целесообразно выделить следующие категории документов:

* номенклатурные дела;
* документы входящего учета;
* документы подразделений;
* документы, находящиеся на архивном хранении в подразделении фондов НТД предприятия;
* носители информации средств ЭВТ.

При необходимости можно выделить также другие категории документов. Например, документы, отражающие взаимоотношения с собственником, с финансирующими организациями (Министерство, банки), материалы информационного обмена и т. п.

**Порядок доступа на совещание по вопросам, содержащим сведения, являющиеся «Конфиденциальной информацией»**

Разрешение на проведение совещаний могут давать руководитель предприятия, его заместители, руководители подразделений, руководители работ. В этой связи необходимо установить и отразить в Разрешительной системе уровень полномочий каждого руководителя.

Руководитель, давший разрешение на проведение совещания, назначает ответственного за его проведение. Ответственный за проведение совещания составляет список его участников и утверждает у руководителя, давшего разрешение на проведение.

В случае, если сотрудник предприятия или представитель другого предприятия приглашаются для обсуждения отдельного вопроса повестки, то об этом делается отметка в списке.

На совещание пропускаются только те лица, которые значатся в списке.

К участию в совещании должны привлекаться только те работники предприятия и представители других предприятий, которые ведут работы по обсуждаемым вопросам и имеют к ним непосредственное отношение.

Целесообразно, чтобы руководитель, открывая совещание, напомнил участникам о необходимости сохранения коммерческой тайны, а также уточнил, какие конкретно сведения являются охраняемыми.

Необходимо также позаботиться, чтобы в ходе совещания охраняемая информация не могла быть получена из-за пределов помещения, в котором проводится совещание. Речь идет о возможности применения визуально-оптических, акустических и др. технических средств, которые могут быть установлены заинтересованными лицами как в самом помещении, так и за его пределами.

Ответственность за соблюдение требований по защите коммерческой тайны правомерно возложить на руководителя, организовавшего совещание.

**Контрольные вопросы:**

1. Что такое разрешительная система? Каковы ее назначение и цели?
2. Как выдаются разрешения на доступ сотрудников предприятия к сведениям, составляющим конфиденциальную информацию?
3. Каков порядок доступа на совещание по вопросам, содержащим сведения, являющиеся «Конфиденциальной информацией»?

**Самостоятельная работа №8** – Защита конфиденциальной информации при обработке и хранении ее в автоматизированных системах.

Основными методами защиты информации в АС являются:

* физическая охрана средств вычислительной техники (СВТ) (устройств и носителей информации), предусматривающая наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и/или специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;
* использование средств вычислительной техники (СВТ) в специально защищенном от ПЭМИН и НСД исполнении;
* использование сертифицированных средств защиты; проведение специальных исследований и контроль СВТ с целью исключения непредусмотренных включений и добавок;
* снижение (исключение) побочных электромагнитных излучений от СВТ;
* снижение (исключение) наводок побочных электромагнитных излучений от СВТ на вспомогательные технические средства (ВТС);
* снижение (исключение) информативности сигналов побочных электромагнитных излучений и наводок с использованием систем активной защиты (генераторов шума);
* идентификация и проверка подлинности (аутентификация) пользователей и других ресурсов АС (программно-аппаратных средств);
* персональный допуск пользователей к работе в АС и ее ресурсам, включая взаимодействие с другими ресурсами АС;
* надзор за деятельностью пользователей в АС и ее учет, включая средства обеспечения персональной ответственности. пользователей за свои действия в АС;
* проверка целостности (отсутствия вредных изменений) ресурсов АС, включая средства защиты информации;
* использование криптографических средств защиты информации, находящейся в оперативной и внешней памяти ЭВМ и на различных носителях, а также передаваемой по линиям связи;
* применение методов защиты от копирования файлов АС;
* периодическое и динамическое тестирование и контроль работоспособности средств защиты, их оперативное восстановление.

В практике защиты конфиденциальной информации АС от перехвата за счет ПЭМИН применяются следующие методы защиты:

1. Применение средств вычислительной техники в защищенном от

ПЭМИН исполнении.

2. Реализация объектовых мер и средств защиты.

3. Использование специальных организационных мероприятий по защите информации от ПЭМИН.

4. Использование технических средств защиты. Наибольшая эффективность защиты от ПЭМИН достигается комплексным сочетанием перечисленных методов в рамках системы защиты информации от ПЭМИН. Выбор методов защиты коммерческой информации в АС от ПЭМИН необходимо проводить с учетом их технико-экономической целесообразности и анализа конкретных условий АС. Разработку системы защиты информации от ПЭМИН в АС должны проводить соответствующие специалисты или специализированные предприятия, имеющие лицензию на данный вид деятельности.

Возможность применения СВТ в защищенном исполнении рассматривается на начальных этапах создания СЗИ. При положительном решении оформляется соответствующий заказ на приобретение таких СВТ у их производителя. При отсутствии требуемых отечественных СВТ в защищенном исполнении следует ориентироваться на СВТ зарубежного производства, выпускаемых с учетом технологии ТЕМРЕ5Т. СВТ зарубежного производства, предназначенные для обработки конфиденциальной информации, следует использовать в АС после проведения специальных проверок на предмет отсутствия в них непредусмотренных включений и добавок. Такие проверки проводят специализированные предприятия, имеющие соответствующую лицензию.

В случае отсутствия СВТ в защищенном исполнении в АС или недостаточности их характеристик по защищенности на основании аналитического обследования АС рассматривается применение объектовых, мер по защите от ПЭМИН. Такие меры могут предусматривать:

создание контролируемой зоны СВТ (территории) в пределах которой исключается или значительно затрудняется перехват сигналов ПЭМИН;

создание специальной зоны, в пределах которой запрещается размещение вспомогательных технических средств (ВТС), исключаются или значительно снижаются наводки на эти средства, исключается (затрудняется) постороннее к ним подключение. ВТС (телефонные средства и системы, цепи освещения, трубопроводы и металлоконструкции, средства и системы кондиционирования, средства охраны и сигнализации и т.п.), имеющие выход за пределы контролируемой зоны, необходимо удалять от основных технических средств;

организацию питания и заземления СВТ, дооборудование помещений, специальное размещение и монтаж СВТ и ВТС, снижающие ПЭМИН.

При недостаточности объектовых мер рекомендуется предусматривать меры организационного характера, включающие организацию охраны и контроля доступа к зонам размещения СВТ и ВТС, проверку цепей и коммуникаций на предмет отсутствия непредусмотренных отводок и подключений и т. п.

Наиболее распространенной системой технической защиты от ПЭМИН является система, которая использует активный метод зашумлению побочных электромагнитных излучений от электронной вычислительной техники (ЭВТ) и наводок в процессе обработки защищаемой информации. Для такой защиты используются специально разработанные генераторы шума с использованием специальной системы антенн. Генераторы устанавливаются в помещениях, где обрабатывается защищаемая информация и включается до начала обработки информации на ЗВТ. Для исключения информативности наводок на ВТС к последним подключается антенная система генераторов шума.

Создание системы активной защиты (САЗ) проводится с использованием специальных изделий и устройств, примером которых являются САЗ «Волна-ЗМ» и «Вектор-4». Требования и рекомендации по изделиям «Волна-ЗМ» и «Вектор-4» содержатся в их проектной документации (издание СНПО «ЭЛЕРОН») и в отраслевых материалах ОРТМ ЭВТ-81.

**Контрольные вопросы:**

* 1. Какие методы защиты информации в АС вам известны?
  2. Что из себя представляет метод «зашумления»?
  3. Какие системы активной защиты вам известны?

**Самостоятельная работа №9**  – Способы несанкционированного доступа к конфиденциальной информации в компьютерных системах и защиты от него.

Основные способы несанкционированного доступа к информации

• непосредственное обращение к объекту с конфиденциальной информацией (например, с помощью управляемой пользователем программы, читающей данные из файла или записывающей их в него);

• создание программных и технических средств, выполняющих обращение к объекту в обход средств защиты (например, с использованием случайно или намеренно оставленных разработчиком этих средств, так называемых люков);

• модификация средств защиты для осуществления несанкционированного доступа (например, внедрение программных закладок);

• внедрение в технические средства СВТ или АС программных или технических механизмов, нарушающих структуру и функции этих средств для осуществления несанкционированного доступа (например, путем загрузки на компьютере иной, незащищенной операционной системы).

**Модель нарушителя**

• нарушитель имеет доступ к работе со штатными средствами КС;

• нарушитель является специалистом высшей квалификации (знает все о КС и, в частности, о системе и средствах ее защиты).

Можно выделить следующие уровни возможностей нарушителя, предоставляемые ему штатными средствами КС (каждый следующий уровень включает в себя предыдущий):

1)запуск программ из фиксированного набора (например, подготовка документов или получение почтовых сообщений);

2)создание и запуск собственных программ (возможности опытного пользователя или пользователя с полномочиями отладки программ);

3)управление функционированием КС — воздействие на ее базовое программное обеспечение, состав и конфигурацию КС (например, внедрение программной закладки);

4)весь объем возможностей лиц, осуществляющих проектирование, реализацию и ремонт средств КС, вплоть до включения в состав КС собственных СВТ с новыми функциями.

**Система разграничения доступа как основное направление обеспечения защиты от НСД**

К основным функциям СРД относятся:

• реализация правил разграничения доступа субъектов и их процессов к информации и устройствам создания ее твердых копий;

• изоляция процессов, выполняемых в интересах субъекта доступа, от других субъектов;

• управление потоками информации в целях предотвращения ее записи на носители несоответствующего уровня конфиденциальности;

• реализация правил обмена информацией между субъектами в компьютерных сетях.

К функциям обеспечивающих средств для СРД относятся:

• идентификация и аутентификация субъектов и поддержание привязки субъекта к процессу, выполняемому для него;

• регистрация действий субъекта и активизированного им процесса;

• исключение и включение новых субъектов и объектов доступа, изменение полномочий субъектов;

• реакция на попытки несанкционированного доступа (сигнализация, блокировка, восстановление объекта после несанкционированного доступа);

• учет выходных печатных форм в КС;

• контроль целостности программной и информационной части СРД и обеспечивающих ее средств.

К основным биометрическим характеристикам пользователей КС, которые могут применяться при их аутентификации, относятся:

• отпечатки пальцев;

• геометрическая форма руки;

• узор радужной оболочки глаза;

• рисунок сетчатки глаза;

• геометрическая форма и размеры лица;

• тембр голоса;

• геометрическая форма и размеры уха и др.

Наиболее распространенными являются программно-аппаратные средства аутентификации пользователей по их отпечаткам пальцев.

**Контрольные вопросы:**

1. Перечислите известные вам способы несанкционированного доступа к информации.
2. Какие модели нарушителя вы знаете?
3. Каковы основные функции НСД?
4. Какие биометрические характеристики можно применять для аутентификации?

СПИСОК ЛИТЕРАТУРЫ

1. Конституция Российской Федерации.
2. Концепция национальной безопасности Российской Федерации (утверждена Указом Президента РФ от 17 декабря 1997 г. N 1300).
3. "Доктрина информационной безопасности Российской Федерации", утверждена Президентом Российской Федерации 9.09.2000 г. № Пр.-1895.
4. Закон Российской Федерации от 21 июля 1993 г. N 5485-1 "О государственной тайне" (с изменениями от 6 октября 1997 г.)
5. Федеральный закон Российской Федерации от 20.02.95 № 24-ФЗ "Об информации, информатизации и защите информации"
6. Федеральный Закон Российской Федерации от 16.02.95 № 15-ФЗ "О связи".
7. Закон Российской Федерации от 19 февраля 1993 г. N 4524-I "О федеральных органах правительственной связи и информации".
8. Закон Российской Федерации от 5 марта 1992 г. N 2446-I "О безопасности".
9. Федеральный закон от 3 апреля 1995 г. N 40-ФЗ "Об органах федеральной службы безопасности Российской Федерации".
10. Федеральный закон Российской Федерации от 4 июля 1996 г. N 85-ФЗ "Об участии в международном информационном обмене".
11. Указ Президента Российской Федерации от 17.12.97 г. № 1300 "Концепция национальной безопасности Российской Федерации" в редакции указа Президента Российской Федерации от 10.01.2000 г. №24.
12. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.
13. ГОСТ Р 6.30-97. Унифицированная система организационно-распорядительной документации.
14. Указ Президента Российской Федерации от 6 марта 1997 г. N 188 "Об утверждении перечня сведений конфиденциального характера".
15. Перечень сведений, отнесенных к государственной тайне в редакции Указов Президента РФ от 24.01.98 г. №61, от 06.06.01 г. № 659.
16. Положение о лицензировании деятельности предприятий и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, утвержденное Постановлением Правительства Российской Федерации № 333 от 15.04.95 г.
17. Каторин Ю.Ф., Куренков Е.В., Лысов А.В., Остапенко А.Н. "Большая энциклопедия промышленного шпионажа" // СПб.: ООО "Издательство Полигон", 2000
18. Требования к содержанию и порядку разработки Руководства по защите информации от технических разведок и от ее утечки по техническим каналам на объекте, одобренные решением Гостехкомиссией России № 42 от 03.10.95 г.
19. Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам (утвержденные Решением Гостехкомиссии России от 23.05. 97 г. № 55).
20. Специальные требования и рекомендации по технической защите конфиденциальной информации (одобрены решением коллегии Гостехкомиссии России от 27.03.2002 г. № 7.2)
21. Положение по аттестации объектов информатизации по требованиям безопасности информации (утверждено председателем Гостехкомиссии России 25.11.94 г.).
22. Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденное Постановлением Правительства Российской Федерации № 912-51 от 15.09.93 г.
23. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации // Руководящий документ, утвержден Председателем Государственной технической комиссии при Президенте Российской Федерации.
24. Максимов Ю.Н. и др. Защита информации в системах и средствах информатизации. СПб.: ВИКА, 1996. - 113 с.
25. Хорев А.А. Способы и средства защиты информации. М.: МО РФ, 1998. - 316 с.
26. Шиверский А.А. Защита информации: проблемы теории и практики. - М.: Юрист, 1996. - 112 с.
27. Д. Халяпин, В. Ярочкин. Основы защиты информации. Служба безопасности предприятия, изд. ИПКИР, 1993, 47 с.
28. В. Ярочкин. Способы несанкционированного доступа к объектам и источникам конфиденциальной информации, изд. ФЗИ РГГУ, 1993, 66 с.
29. В.Н.Алексеенко. Современная концепция комплексной защиты. Технические средства защиты. М., МИФИ, 1994, 37с.
30. М. Вус, В. Морозов. Информационно-коммерческая безопасности: защита коммерческой тайны, Санкт-Петербург, 1993, 52 с.
31. А. Жуков. Все о защите коммерческой тайны, Москва, 1992, 55 с.
32. А. Левин. Секрет фирмы, Машиностроение, 1993 (2‑е изд.), 107 с.
33. В. Самотуга, С. Андреев. Коммерческая тайна и ее защита, Внешторгиздат, 1992, 80 с.
34. Сборник "Коммерческая тайна. Извлечения из законодательных и других нормативных актов СССР и РСФСР", 1991, 41 с.
35. Сборник "Защита коммерческой информации в условиях рыночной экономики и внешнеэкономической деятельности", Москва, 1992, 95 с.
36. Сборник "Защита коммерческой информации. Коммерческая тайна. Сборник нормативных и справочных материалов" (выпуск 1‑й), Клен, 1991, 32 с.