













Презентация ОДО

**« Работа с документами, содержащими
конфиденциальную информацию »**

Содержание

- Введение 
- Виды конфиденциальных документов 
- Общие понятия информационных ресурсов 
- Перечень конфиденциальных сведений 
- Перечень документов архива, содержащих конфиденциальную информацию 
- Организация работы с конфиденциальными документами 
- Понятие системы защиты информации 
- Элементы системы защиты информации 
- Объекты угроз конфиденциальной информации архива 
- Угрозы конфиденциальной информации 
- Заключение 
- Список литературы 

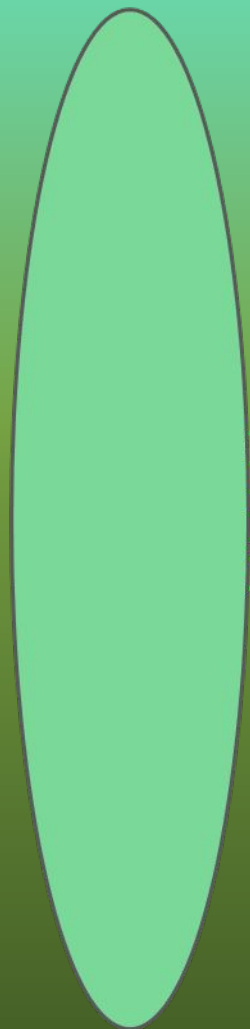


Виды конфиденциальных документов



Общие понятия Информационных ресурсов

- Персональные – сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в СМИ в установленном порядке.
- Профессиональная тайна – сведения, связанные с профессиональной деятельностью, доступ к которым ограничен законами.
- Коммерческая тайна – сведения, связанные с коммерческой деятельностью, доступ к которым ограничен законами.
- Производственная тайна – сведения о сущности изобретения полезной модели или промышленного образца до официальной публикации информации о них.
- Служебная тайна – служебные сведения, доступ к которым ограничен органами государственной власти.
- Судебно-следственная информация – сведения, составляющие тайну следственной власти.



Сведения, составляющие персональные данные физических лиц, дела которых находятся на хранении в архиве

Сведения, составляющие персональные данные сотрудников архива

Данные бухгалтерского, налогового и управленческого учета

Плановые и фактические показатели финансово-хозяйственной деятельности архива

Сведения о технологии функционирования охранной и противопожарной системы архива

Сведения о состоянии программного и компьютерного обеспечения архива

Сведения о проведении, повестках дня и результатах служебных совещаний архива

Перечень документов архива, содержащих конфиденциальную информацию

Документы по личному составу и социально-правовые документы, находящиеся на хранении в архиве: личные дела работников, приказы по личному составу и т.д.


Документы по личному составу самого архива (личные дела сотрудников архива; приказы по личному составу и т.д.)

Документация по бухгалтерскому и налоговому учету и отчетности (баланс архива, отчеты, подаваемые в налоговые органы, ведомости начисления заработной платы сотрудникам архива и т.д.)


Документы, отражающие технологию функционирования охранной системы архива

Документы, образующиеся в деятельности сотрудников архива при исполнении запросов социально-правового характера





Организация работы с конфиденциальными документами



- *Конфиденциальные документы подлежат обязательной регистрации в подразделении делопроизводства службы безопасности (в Первом отделе) или в общем делопроизводстве производственного подразделения уполномоченного службой безопасности.*
- *Учет конфиденциальных документов ведется в журналах или карточках отдельного учета другой служебной службы несекретной информации.*
- *Размножение конфиденциальных документов и в типографиях и других множительных участках производится с разрешения и под контролем специально назначенных сотрудников службы безопасности по заказам, подписанным руководителем предприятия.*
- *Снятие рукописных, машинописных, микро – и фотокопий, электрографических и др. копий, а также производство выписок из конфиденциальных документов производится по разрешению руководителя предприятия и подразделения*



Понятие и элементы системы защиты информации

Система защиты информации (СЗИ) – рациональная совокупность направлений, методов, средств и мероприятий, снижающих уязвимость информации и препятствующих несанкционированно доступу к информации, ее разглашению или утечке.

ГОСТ Р50922-96 «Защита информации. Основные термины и определения» закрепляет понятие СЗИ как совокупность органов и/или исполнителей, используемых ими техники информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

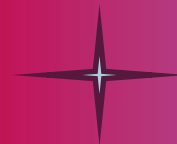
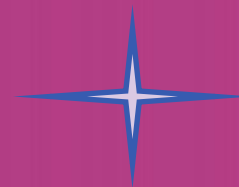
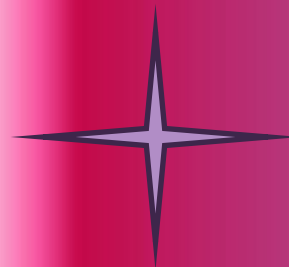


- ♦ *Правовой элемент* - это специальные законы, другие нормативные акты, правила. Обеспечивающие защиту информации на правовой основе;
- ♦ *Организационный элемент* - включает регламентацию производственной деятельности и взаимоотношений исполнителей на нормативной основе;
- ♦ *Инженерно-технический элемент* – это использование различных средств, препятствующих нанесению ущерба защищаемой информации;
- ♦ *Программно-аппаратный и криптографический элемент.*



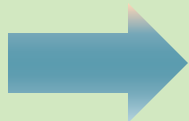
Под объектом защиты надо понимать комплекс физических, аппаратных, программных и документальных средств, предназначенных для сбора, передачи, обработки и хранения информации. Исходя из функций организации, можно установить какая информация создается, обрабатывается, хранится в процессе ее деятельности.

ОБЪЕКТЫ УГРОЗ
КОНФИДЕНЦИАЛЬНО
ИНФОРМАЦИИ
АРХИВА

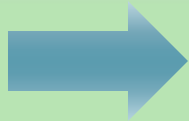




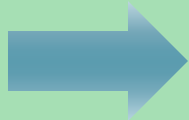
УГРОЗЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ АРХИВА



Нарушение физической ценности – модификация, подделка, уничтожение, потери, ошибки.



Нарушение доступности – блокирование доступа к базам данных архива, в операционную систему, папкам и файлам, содержащим конфиденциальную информацию.



Нарушение доверенности – фальсификация, подделка, как документа, так и его части.



Ввод в компьютерные системы разрушительных программных средств, вирусов.



Несчастные случаи: пожары, аварии, взрывы.



Ошибки в процессе обработки информации: сбои в работе технических и программных средствах; систем питания и жизнеобеспечения; ошибки пользователей (сотрудников архива).



Для эффективного построения СЗИ применяются комплексный подход, поэтому необходимо учитывать вероятность возникновения угроз, цели злоумышленников по отношению к ценной информации определить ценность самой информации. Нельзя забывать и о благонадежности персонала. Человеческий фактор всегда присутствует и является одним из главных. В этой связи должны проводиться беседы с персоналом на предмет важности защиты информации, организовываться специальные мероприятия, каждый сотрудник должен знать ответственность за нарушение действующего законодательства локальных нормативных актов в области защиты конфиденциальной информации.



СПИСОК ЛИТЕРАТУРЫ

- Корнеев И.К., Степанов Е.А. «Информационная безопасность и защита информации», М.:ИНФОРА-М, 2001.- 299 с;
- Ярочкин В.И. «Информационная безопасность», 3-е изд.-М.: Академический Проект: Трикста.-2005.-544 с.
- Степанов Е.А. «Организация доступа персонала к конфиденциальным документам», Секретарское дело. 1998. № 2;
- Сукач А.Н «Организационные мероприятия по защите информации», Отдел кадров.- 2006.-№ 3.-С.12.

