Цель работы:

- исследование терминологической базы

- закрепление знаний основного понятийного аппарата, применяемого в области защиты информации

- формирование навыка работы с нормативными документами по исследуемому вопросу

- анализ угроз информационной безопасности

Ход выполнения задания

1. Определение требований к защите информации

Объект защиты информации: материалы для служебного пользования на твёрдых носителях в производстве.

Перечень защищаемой информации:

1) Документы по личному составу (Трудовые договоры, личные карточки сотрудников, счета работников)
2) Личные дела сотрудников
3) Журналы учета рабочего времени
4) Деловые переписки

Материалы для служебного пользования на твёрдых носителях в производстве являются информацией ограниченного доступа, являющихся персональной и коммерческой тайной.

В соответствии Правительства ФЗ №152 «О персональных данных», ФЗ №98 «О коммерческой тайне» и с постановлением Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» необходимо определить защиту 3-го уровня, так как для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора.

В таком случае необходимо выполнение следующих требований:

А) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

Б) обеспечение сохранности носителей персональных данных;

В) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

Г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;

Необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение персональных данных в информационной системе.

При режиме коммерческой тайны в соответствии с ФЗ №98 «О коммерческой тайне», необходимо:

• обеспечить ознакомление работника с тем, что он будет работать с документами, являющимися коммерческой тайной;

• определить группу лиц, имеющих доступ к этим документам;

• классифицировать документы, содержащие коммерческую информацию, по степени секретности и срокам хранения.

Федеральный закон от 22.10.2004 N 125-ФЗ «Об архивном деле в Российской Федерации» говорит о том, что документы должны храниться в условиях, обеспечивающих их защиту от повреждений, вредных воздействий окружающей среды и исключающих утрату документов. В этом случае необходимо соблюдать:

• световой режим

• температурно-влажностный режим

• санитарно-гигиенический режим

• охранный режим

2. Классификация автоматизированной системы

В соответствии с условием, что пользователи имеют одинаковые права доступа ко всей информации АС, наш класс – 2Б.

Подсистемы и требования	Классы								
	1А	1Б	1В	1Г	1Д	2А	2Б	3А	3Б
1. Подсистема управления доступом									
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:									
В систему	+	+	+	+	+	+	+	+	+
К терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-	+	+	+	+	+	-	-	-
к программам	-	+	+	+	+	+	-	-	-
к томам, каталогам, файлам, записям, полям записей	-	+	+	+	+	+	-	-	-
1.2 Управление потоками информации	-	-	+	+	+	+	-		
2. Подсистема регистрации и учета									
2.1. Регистрация и учёт:									
входа (выхода) субъектов доступа в (из) систему (узел сети)	+	+	+	+	+	+	+	+	+
выдачи печатных (графических) выходных документов	-	+	+	+	+	+	-	-	+
запуска (завершения) программ и процессов (заданий, задач)	-	+	+	+	+	+	-	-	-
доступа программ субъектов доступа к	-	+	+	+	+	+	-	-	-

защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи									
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	-	+	+	+	+	+	-	-	-
изменения полномочий субъектов доступа	-	-	+	+	+	-	-	-	-
создаваемых защищаемых объектов доступа	-	-	+	+	+	+	-	-	-
2.2. Учет носителей информации	+	+	+	+	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-	+	+	+	+	+	-	-	+
2.4. Сигнализация попыток нарушения защиты	-	-	+	+	+	-	-	-	-
3. Криптографическая подсистема									
3.1. Шифрование конфиденциальной информации	-	-	-	+	+	+	-	-	-
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	-	-	-	-	+	-	-	-	-
3.3. Использование аттестованных (сертифицированных) криптографических средств	-	-	-	+	+	+	-	-	-
4. Подсистема обеспечения целостности									
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+	+	+	+	+
4.3. Наличие администратора (службы) защиты информации в АС	-	+	+	+	+	+	-	-	-
4.4. Периодическое тестирование СЗИ НСД	+	+	+	+	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД	+	+	+	+	+	+	+	+	+
4.6. Использование сертифицированных средств защиты	-	-	+	+	+	+	-	-	+

3. Определение факторов, влияющих на требуемый уровень защиты информации

Конфиденциальность:

1) Несанкционированный доступ

2) Кража

3) Хищение

4) Утечка

Целостность:

1) Пожар

2) Затопление

3) Иные стихийные бедствия

4) Нарушение семантатики

Доступность:

1) Уничтожение информации

2) Приведение носителей в непригодное состояние

3) Замыкание электрического замка

4. Способы и средства защиты инфы

Целостность:

1) Установка системы пожаротушения на порошковой основе (или иные средства, не повреждающие носители). К примеру, можно использовать охранно-пожарную систему С2000 на порошковой основе.

2) Расположение архива на средних этажах и в местах, где невозможно затопление сверху.

3) Хранение документов должно соответствовать температурно-влажностным нормам. Например, можно использовать увлажнитель воздуха гт-1,6 от производителя par-tuman.

4) Отсутствие окон в архиве

Конфиденциальность:

1) Наличие лиц, ответственных за доступ сотрудников к архиву. (Выполнение подсистема обеспечения целостности)

2) Использование системы специальных пропусков для регистрации посещения и выхода сотрудника. (Выполнения условия идентификации, проверки подлинности и контроля доступа субъектов) К примеру система специальных пропусков от компании «PocketKey

3) Наличие лиц, ведущий аудит выдачи документов (Выполнения условий Регистрация и учёта: входа (выхода) субъектов доступа в (из) систему (узел сети) носителей информации, а также учёта носителей информации).

Доступность:

1) Расположение внутри архива охранной сигнализации. Например, можно использовать охранную сигнализацию «Onviz Smart Pro» от компании «Onviz»

2) Опечатывание помещения в нерабочее время

5. Рекомендации по увеличению уровня защищенности

1) Проведение мероприятий технических мероприятий по проверке защитного оборудования раз в год-полутора.

2) Проведение инструктажа персонала по работе с конфиденциальной информацией раз в 6 месяцев

Вывод

Была проведена работа с нормативными документами по исследуемому объекту защиты и по исследованию терминологической базы, закрепили знания основного понятийного аппарата, применяемого в области защиты информации, проанализировали угрозы информационной безопасности.

Была создана система, соответствующая требованиям ФЗ №152 «О персональных данных», ФЗ №98 «О коммерческой тайне» и с постановлением Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»