Разработка Концепции обеспечения информационной безопасности для предприятия

Содержание

• Общие положения

1 Описание объекта защиты

 Назначение и основные функции информационной системы

 Группы задач, решаемых в информационной системе

 Классификация пользователей системы

 Организационная структура обслуживающего персонала

2 Структура и состав комплекса программно-технических средств

 Корпоративная сеть предприятия

 Серверы

 Рабочие станции

 Линии связи и активное сетевое оборудование

3 Виды информационных ресурсов, хранимых и обрабатываемых в системе

 Структура информационных потоков

 Внутренние информационные потоки

 Внешние информационные потоки

 Характеристика каналов взаимодействия с другими системами и точек входа

4 Основные факторы, влияющие на информационную безопасность предприятия (рост преступности, увеличение объёма информации …)

5 Основные принципы обеспечения информационной безопасности (надёжность, комплексность, равнопрочность, простота …)

6 Организация работ по защите информации (кто занимается ЗИ, права и обязанности, структура)

7 Меры обеспечения информационной безопасности

 Меры обеспечения информационной безопасности организационного уровня

 Меры обеспечения информационной безопасности программно-аппаратного уровня

 Меры обеспечения информационной безопасности инженерно-технического уровня

8 Порядок взаимодействия с другими подразделениями (отдел кадров, СБ …)

9 Порядок категорирования защищаемой информации (что относится к защищаемой информации, порядок отнесения сведений к КТ, общий перечень сведений КТ …)

10 Модель нарушителя информационной безопасности

 Внутренние нарушители

 Внешние нарушители

11 Модель угроз информационной безопасности

11.1 Защита информационных компонентов и группы угроз (объекты защиты и основные виды угроз)

 Угрозы, реализуемые с использованием технических средств

 Угрозы, реализуемые с использованием программных средств

 Угрозы утечки информации по техническим каналам связи

12 Требования по обеспечению информационной безопасности

12.1 Состав основных подсистем СОИБ

 Требования к подсистеме управления политикой безопасности (для чего предназначена что должна делать,)

 Требования к подсистеме анализа и управления рисками

 Требования к подсистеме идентификации и аутентификации

 Требования к подсистеме разграничения доступа

 Требования к подсистеме аудита

 Требования к подсистеме антивирусной защиты

 Требования к подсистеме фильтрации контента

 Требования к подсистеме предотвращения утечки информации по техническим каналам

 Требования по физической защите

13 Ответственность сотрудников за нарушение безопасности

14 Механизм реализации концепции