Основы кибербезопасности и механизмы ее соблюдения

1. Основы информационной безопасности

Понятие «информационная безопасность»

- Информационная безопасность государства заключается в невозможности нанесения ущерба деятельности государства по выполнению функций в информационной сфере по управлению обществом и поддержанием порядка.

Государственная политика в области информационной безопасности

- Нормативно-правовая база
- Регламентация доступа к информации
- Юридическая ответственность за сохранность информации
- Контроль за разработкой и использованием средств защиты информации
- Предоставление гражданам доступа к мировым информационным системам

Информационная война

- Распространение ложной информации
- Манипулирование личностью.
- Разрушение традиционных духовных ценностей
- Навязывание инородных духовных ценностей
- Искажение исторической памяти народа
- Кибертерроризм

Национальные интересы в информационной сфере

- Обеспечение прав и свобод граждан на получение и распространение информации
- Обеспечение деятельности субъектов национальных интересов в информационной инфраструктуре общества (овладение надлежащей информацией и удовлетворение потребителей по ее использованию)

СМИ и информационная безопасность

- Реализация потенциальной возможности манипулирования населением с помощью СМИ .
- Изменение акцентов в распространяемой информации.
- Распространение «правдоподобной» информации под видом истинной.
- Навязывание оценок событиям в интересах конкретных общественных групп.

Угрозы информационной безопасности

- 1. Уничтожение информационных объектов
- 2. Утечка информации
- 3. Искажение информации
- 4. Блокирование объекта информации

Объекты защиты информации

- Владельцы и пользователи
- Носители и средства обработки
- Системы связи и информатизации
- Объекты органов управления

Конфиденциальность информации

- Субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы сохранять указанную информацию в тайне от субъектов,не имеющих полномочий доступа к ней.

Целостность информации

- Существование информации в неискаженном виде, т.е. в неизменном по отношению к некоторому фиксированному ее состоянию.

Доступность информации

- Свойство системы, характеризующееся способностью обеспечивать своевременный и беспрепятственный доступ к информации субъектов соответствии с запросами

Аппаратно-программные средства ЗИ

- Системы идентификации и аутентификации пользователей
- Системы шифрования данных на дисках
- Системы шифрования данных, пересылаемых по сети
- Системы аутентификации электронных данных
- Средства управления ключами

Угрозы проникновения

- Маскарад-пользователь маскируется под другого пользователя.
- Обход защиты-использование слабых мест в системе безопасности с целью получения доступа.
- Нарушение полномочий-использование ресурсов не по назначению.
- Троянские программы-программы, содержащие программный код, при выполнении которого нарушается функционирование системы безопасности.

Противодействие техническим средствам разведки

- Формирование системы противодействия ТСР
- Скрытие демаскирующих признаков
- Противодействие распознаванию объекта
- Техническая дезинформация (подавление демаскирующих сигналов)
- Контроль эффективности противодействия ТСР

Задание Необходимо провести анализ защищенности объекта защиты информации по следующим разделам:

1. Виды возможных угроз 2
2. Характер происхождения угроз
3. Классы каналов несанкционированного получения информации
4. Источники появления угроз
5. Причины нарушения целостности информации
6. Потенциально возможные злоумышленные действия
7. Определить класс защищенности автоматизированной системы