|  |  |  |  |
| --- | --- | --- | --- |
| 1. (1) Информация, (2) ИБ, (3) угрозы без. Инф. (4).Класс. угроз по природе возн. И степени преднамеренности (5) Класс. Угроз по источнику (6)Класс. угроз по положению источника. (7) Класс. угроз по степени активности ИС (8) Класс. Злоумышленников (9).Осн направления угроз.  2. (10).Причины, виды и каналы утечки информации (11.)Основные положения «Доктрины информационной безопасности».  3.  4.  5.  6.  7.  8.  9.  10.  11. | 1. **Информация** – сведения о мире, отраженные на мат-ых носителях для получения знаний и практических решений.  Свойства:  - Обьективность – сущ. Вне и независимо от человеческого сознания  - Достоверность – отр. Истинное положение дел  - Полнота – инф. достаточно для понимания и принятия решений  - Точность – степень ее близости к реальному положению дел.  - Ценность – по отношению к нуждам ее потребителей. Оцен. по задачам.  - Актуальность – важность для наст. времени.  **2. ИБ** - защищенность информации и поддерживающей инфраструктуры от различных воздействий, которые могут нанести ущерб участникам информационной деятельности.  Защита инф. – комплекс мероприятий, направленных на обеспечение информационной безопасности.  3. **Угрозы безопасности информации.**  Угроза - потенциально возможное событие, которое может привести к нанесению ущерба чьим-либо интересам.  - Целостности – несанкционированное искажение инф.  - Доступность – неспособность обеспеч. Своевр. Доступ к инф.  - Конфиденциальности – инф. известна тому, у кого нет полномочий доступа к этой инф.  **4.Классификация угроз безопасности по природе возникновения и степени преднамеренности.**  По природе возникновения:  - Естественные угрозы (Природа, физические явления)  - Искусственные угрозы (Деятельность человека)  По степени преднамеренности:  - Непреднамеренные (Ошибки персонала, халатность)  - Преднамеренные (Шпионаж, диверсия и прочее) | 2. **10.Причины, виды и каналы утечки информации**  Причины:  - несоблюдение норм эксплуатации АС  - ошибки проектирования АС и систем защиты  - ведение разведок противником  Виды утечки информации:  - разглашение  - несанкционированный доступ  - кража (работа разведки)  Канал утечки информации – путь распространения информации в руки злоумышленника посредством манипуляций с её носителем.  **11.Основные положения «Доктрины ИБ».**  Доктрина ИБ РФ – совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения ИБ РФ.  Основные положения:  1)*Нац. Интересы РФ в информационной сфере и их обеспечение*  *Совокупность интересов личности, общества и государства.*  Личность:  Обеспечение конституционных прав на доступность и использование информации в рамках закона, а так же защиты личной информации.  Общество:  Соблюдение интересов личности, демократического строя, создании правового социального государства.  Государство:  Развитие информационной инфраструктуры для реализации конституционных прав и свобод в области получения информации, для развития и укрепления страны, а также укрепления её безопасности. | 3. |
| 4. | 5. | 6. | 7. |
| 3. | 2. | 1. **5.Классификация угроз безопасности по непосредственному источнику угроз.**  - Природная стихия (Ураган, землетрясение и т.д.)  - Человек (Внедрение агентов, разглашение, утрата и т.д.)  - Санкц.ПО (Вирусы, некомпетентное исп. ПО и т.д.)  - Несанкционированные ПО (Игры, редакторы и т.д. (Расход ресурсов))  **6.Классификация угроз безопасности по положению источника угроз**  - Не контролируемая зона (Перехват линий связи, волн, излучений и т.д.)  - Контролируемая зона (Хищение, отключение, вывод из строя и т.д.)  - Внутри АС (Разработка систем и программ, нарушающих работу АС)  **7. Классификация угроз безопасности по степени активности информационной системы.**  - Независимы от активности АС (вскрытие шифров, хищение носителей)  - В процессе работы АС (Распространение, работа вирусных программ)  **8.Классификация злоумышленников**  - Разработчик ИВС (Владеет всей информацией о программе)  - Сотрудник обслуживающего персонала (Знает всё о работе системы)  - Пользователь (Знает о структуре ИВС)  - Постороннее лицо (Шпионаж, диверсия)  **9.Основные направления реализации информационных угроз.**  - прямое обращение к объектам доступа  - создание ПО, обр-ихся к объектам доступа (в обход защиты)  - модификация защиты для реализации угроз  - внедрение ПО или механизмов для нарушения целостности АС | 0. |
| 7. | 6. | 5. | 4. |