1. Под безопасностью информационной системы понимается защищенность системы от случайного или преднамеренного вмешательства в нормальный процесс её функционирования, от попыток хищения информации, модификации и нарушения её компонентов.

2. **Информационная** **безопасность** (**ИБ**) – это состояние информационной системы, при котором она наименее восприимчива к вмешательству и нанесению ущерба со стороны третьих лиц. Безопасность **данных** также подразумевает управление рисками, которые связаны с разглашением информации или влиянием на аппаратные и программные модули защиты.

**Корпоративные** **информационные** **системы** (**КИС**) в целом можно рассматривать как управленческую идеологию, которая реализована на основе **информационных** **систем** и использует ключевые бизнес-стратегии организации или предприятия. Эти **системы** предназначены в первую очередь для упрощения выполнения задач по систематизации информации и автоматизации различных процессов, связанных с хранением и обработкой данных.

3. **По цели воздействия**- (Нарушение конфиденциальности, Нарушение работоспособности, Нарушение целостности)

**По характеру воздействия**- (Активные(кража или изменение информации), Пассивные(наблюдение за прохождением ниформации))

**По характеру возникновения**- (Случайные(Сбои аппаратуры, ошибки в ПО и ошибки обслуживающего персонала), Преднамеренные(связанные с целенаправленными действиями нарушителя))

4. К числу основных методов реализации угроз информационной безопасности относятся:

•определение типа и параметров носителей информации;

•получение информации о программно-аппаратной среде, типе и параметрах средств вычислительной техники, типе и версии операционной системы, составе прикладного программного обеспечения;

•получение детальной информации о функциях, а также получение данных о применяемых системах защиты;

•определение способа представления информации;

• определение содержания данных на качественном уровне (применяется для мониторинга и для дешифрования сообщений);

•хищение (копирование) машинных носителей информации, содержащих конфиденциальные данные

•уничтожение средств вычислительной техники и носителей информации;

•несанкционированный доступ пользователя к ресурсам в обход или путем преодоления систем защиты с использованием специальных средств, приемов, методов;

5. **Информационная система**- система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы, которые обеспечивают и распространяют информацию.

6. **Информационные ресурсы**- являются источником информации, представляют собой отдельные документы и массивы документов в информационных системах.

7. **Основу политики безопасности** составляет способ управления доступом, определяющий порядок доступа субъектов системы к объектам системы. Название этого способа, как правило, определяет название политики безопасности. Для изучения свойств способа управления доступом создается его формальное описание – математическая модель.

9. **Объект защиты информации** - информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации. В соответствии с данным определением можно классифицировать объекты защиты.

10. **Информационными процессами**- называют такие процессы, которые связаны с изменением информации или действиями с использованием информации. Есть несколько основных информационных процессов: сбор информации; представление информации; обработка информации; хранение информации; передача информации.

11. **Информационная система**- система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы, которые обеспечивают и распространяют информацию.

12. **Информационные ресурсы**- являются источником информации, представляют собой отдельные документы и массивы документов в информационных систем