Первая пара:

1. Угроза – это действие, которое потенциально может привести к нарушению информационной безопасности.
2. Уязвимость – слабое место в информационной системе, которое может привести к нарушению безопасности путём реализации некоторой угрозы.
3. Злоумышленник – тот, кто предпринимает попытку реализовать угрозу.
4. Вероятность реализации угрозы – степень возможности реализации угрозы через данную уязвимость в тех или иных условиях в процентах.
5. Критичность реализации угрозы – степень влияния реализации угрозы на ресурс. То, как сильно реализация повлияет на работу ресурса. Оценивается в процентах и состоит из критичности по конфидециальности, целостности и доступности (ERc, Eri, ERa).
6. Окно опасности – промежуток времени от момента когда появляется возможность использовать слабое место и до момента, когда пробел ликвидируется.
7. Модель угроз – документ, определяющий перечень и характеристики основных (актуальных) угроз безопасности и уязвимостей при их обработке в ИС, которые должны учитываться в процессе организации защиты информации, проектирования и разработки систем защиты информации, проведения проверок (контроля) защищённости ИС.
8. Цель разработки модели угроз – определение актуальных для конкретной ИС угроз безопасности, источников угроз и уязвимостей. Результаты моделирования должны использоваться в качестве исходных данных для выработки требований ИБ к разрабатываемой системе защиты.
9. Классификация угроз по аспектам ИБ:
   1. Аспекту информационной безопасности
   2. Компонентам информационных систем
   3. Происхождение и способ осуществления
   4. По расположению
   5. Прочие: по способу доступа, по этапу доступа, по текущему месту расположения информации)
10. Классификация угроз по компонентам ИС.
    1. Данные
    2. Программы
    3. Аппаратура
    4. Поддерживающая инфраструктура
11. Классификация угроз по происхождению и способу осуществления.
    1. Преднамеренные
    2. Непреднамеренные
    3. Природные
    4. Техногенные
12. Классификация угроз по расположению источников угроз.
    1. Внутренние
    2. Внешние
13. Угрозы доступности данных возникают в том случае, когда объект (пользователь или процесс) не получает доступа к законно выделенным ему службам или ресурсам.
14. Угрозы целостности данных, программ, аппаратуры. Целостность данных и программ нарушается при несанкционированном уничтожении, добавлении лишних элементов и модификации записей о состоянии счетов, изменении порядка расположения данных, формировании фальсифицированных платежных документов в ответ на законные запросы, при активной ретрансляции сообщений с их задержкой.
15. Угрозы конфиденциальности данных и программ реализуются при несанкционированном доступе к данным (например, к сведениям о состоянии счетов клиентов банка), программам или каналам связи
16. Вредоносные программы – специальные программы, такие как логические бомбы, черви, троянские кони и компьютерные вирусы.
17. Информационная безопасность – защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера.
18. Безопасность информации – такое состояние информации, при котором обеспечена её конфиденциальность, целостность и доступность (мейби, перепроверить)
19. Информационные технологии - отвечают за оборудование, разработку программного обеспечения и новые технологии, используемые для обработки информации. (взял из инета, перепроверить)
20. Информационная система – совокупность баз данных и технических средств и технологий для её обработки.
21. Защита информации от утечки – защита информации направленная на защиту от неконтролируемого распространения информации полученной вследствие разглашения или несанкционировнного доступа.
22. Защита информации от несанкционированного воздействия - защита информации от несанкционированного доступа и воздействия лицами, не имеющими на это доступ.
23. Система защиты информации - совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации. (взял из ГОСТа)
24. Виды информации ограниченного доступа. Гостайна и конфиденциальная информация. Вторая содержит персональные данные, проф. данные, коммерческую тайну, тайна следствия и судопроизводства, Служебные сведения, сущность изобретения.
25. Информация и её классификация. Информация бывает публичной и ограниченного доступа. Информация – любые сведения вне зависимости от их формы представления.
26. Основные положения ФЗ-149. осуществлении права на поиск, получение, передачу, производство и распространение информации; 2) применении информационных технологий; 3) обеспечении защиты информации. Взял из самого ФЗ-149
27. Основные положения ФЗ-5485-1. Настоящий Закон регулирует отношения, связанные с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой государственной тайны в интересах обеспечения безопасности Российской Федерации.
28. Основные положения ФЗ-152. отношения, связанные с обработкой персональных данных, хранением.
29. Основные положения ФЗ-63. Настоящий Федеральный закон регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами.

Опрос два

Первая пара:

1. Угроза – это действие, которое потенциально может привести к нарушению информационной безопасности.
2. Уязвимость – слабое место в информационной системе, которое может привести к нарушению безопасности путём реализации некоторой угрозы.
3. Злоумышленник – тот, кто предпринимает попытку реализовать угрозу.
4. Вероятность реализации угрозы – степень возможности реализации угрозы через данную уязвимость в тех или иных условиях в процентах.
5. Критичность реализации угрозы – степень влияния реализации угрозы на ресурс. То, как сильно реализация повлияет на работу ресурса. Оценивается в процентах и состоит из критичности по конфидециальности, целостности и доступности (ERc, Eri, ERa).
6. Окно опасности – промежуток времени от момента когда появляется возможность использовать слабое место и до момента, когда пробел ликвидируется.
7. Модель угроз – документ, определяющий перечень и характеристики основных (актуальных) угроз безопасности и уязвимостей при их обработке в ИС, которые должны учитываться в процессе организации защиты информации, проектирования и разработки систем защиты информации, проведения проверок (контроля) защищённости ИС.
8. Цель разработки модели угроз – определение актуальных для конкретной ИС угроз безопасности, источников угроз и уязвимостей. Результаты моделирования должны использоваться в качестве исходных данных для выработки требований ИБ к разрабатываемой системе защиты.
9. Классификация угроз по аспектам ИБ:
   1. Аспекту информационной безопасности
   2. Компонентам информационных систем
   3. Происхождение и способ осуществления
   4. По расположению
   5. Прочие: по способу доступа, по этапу доступа, по текущему месту расположения информации)
10. Классификация угроз по компонентам ИС.
    1. Данные
    2. Программы
    3. Аппаратура
    4. Поддерживающая инфраструктура
11. Классификация угроз по происхождению и способу осуществления.
    1. Преднамеренные
    2. Непреднамеренные
    3. Природные
    4. Техногенные
12. Классификация угроз по расположению источников угроз.
    1. Внутренние
    2. Внешние
13. Угрозы доступности данных возникают в том случае, когда объект (пользователь или процесс) не получает доступа к законно выделенным ему службам или ресурсам. Технические причины могут быть отказ ИС или поддерживающей инфраструктуры, человеческие факторы.
14. Угрозы целостности данных, программ, аппаратуры. Целостность данных и программ нарушается при несанкционированном уничтожении, добавлении лишних элементов и модификации записей о состоянии счетов, изменении порядка расположения данных, формировании фальсифицированных платежных документов в ответ на законные запросы, при активной ретрансляции сообщений с их задержкой. Угроза целостности бывает данным, программам и аппаратуре. Статическая целостность – неверные данные. А динамическая целостность – нарушение атомарности транзакций, переупорядочение, внесение доп пакетов и т.д.
15. Угрозы конфиденциальности данных реализуются при НСД к данным программам каналам связи
16. Вредоносные программы – специальные программы, такие как логические бомбы, черви, троянские кони и компьютерные вирусы.
17. Информационная безопасность – защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера.
18. Безопасность информации – такое состояние информации, при котором обеспечена её конфиденциальность, целостность и доступность (мейби, перепроверить)
19. Информационная система – совокупность баз данных и технических средств и технологий для её обработки.
20. Защита информации от утечки – защита информации направленная на защиту от неконтролируемого распространения информации полученной вследствие разглашения или несанкционировнного доступа.
21. Защита информации от несанкционированного воздействия - защита информации от несанкционированного доступа и воздействия лицами, не имеющими на это доступ.
22. Риск в сфере ИБ – потенциальная возможность понести убытки из-за нарушения безопасности информационной системы.
23. Подходы к обоснованию проекта подсистемы обеспечения безопасности.
    1. Использовать стандарты при проверке уровня защищённости. Это может быть класс защищенности в соответствии с требованиями руководящих документов Гостехкомиссии РФ (сейчас это ФСТЭК России), профиль защиты, разработанный в соответствии со стандартом ISO-15408, или какой-либо другой набор требований. Критерий достижения цели – удовлетворение этим стандартам. Критерий эффективности – минимальные суммарные затраты на выполнение поставленных функциональных требований. Если уровень защиты четко не задан, определить наиболее эффективный уровень защищённости ИС сложно.
    2. Второй подход связан с оценкой и управлением рисками. Абсолютная защита невозможна. Нужно соблюдать баланс между затратами на защиту и получаемым эффектом, стоимость защиты не должна превышать стоимость защищаемой информации, затраты нарушителя на НСД должны превысить эффект, который он получит при осуществлении НСД.
24. Суть риск-ориентированного подхода при обеспечении ИБ. решения по реализации мер защиты информационной системы принимаются на основе анализа и оценки рисков нанесения ущерба организации.
25. Риск может быть:

− снижен (например, за счет внедрения средств и механизмов защиты, уменьшающих вероятность реализации угрозы или коэффициент разрушительности);

− устранен (за счет отказа от использования подверженного угрозе ресурса);

− перенесен (например, застрахован, в результате чего в случае реализации угрозы безопасности, потери будет нести страховая компания, а не владелец ИС);

− принят. (понимать, что риск взлома (угроза) есть, но считать, что потенциальный ущерб не так велик)

1. Система защиты информации - совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации. (взял из ГОСТа)
2. Виды информации ограниченного доступа. Гостайна и конфиденциальная информация. Вторая содержит персональные данные, проф. данные, коммерческую тайну, тайна следствия и судопроизводства, Служебные сведения, сущность изобретения.
3. Информация и её классификация. Информация бывает публичной и ограниченного доступа. Информация – любые сведения вне зависимости от их формы представления.
4. Основные положения ФЗ-149. осуществлении права на поиск, получение, передачу, производство и распространение информации; 2) применении информационных технологий; 3) обеспечении защиты информации. Взял из самого ФЗ-149
5. Основные положения ФЗ-5485-1. Настоящий Закон регулирует отношения, связанные с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой государственной тайны в интересах обеспечения безопасности Российской Федерации.
6. Основные положения ФЗ-152. отношения, связанные с обработкой персональных данных, хранением.
7. Основные положения ФЗ-63. Настоящий Федеральный закон регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами.