Вопросы к экзамену по дисциплине «Защита информации»
для студентов 4 курса групп ИВТ-41 и ИВТ-42

1. Информационная безопасность (ИБ) – основные понятия и определения, дайте определения следующим понятиям: информация, безопасность, субъекты и объекты безопасности, угроза, уязвимость, атака.
2. Информационная безопасность. Дайте определения составляющим информационной безопасности: конфиденциальность (Confidentiality), целостность (Integrity), доступность (Availability)
3. Информационная безопасность. Дайте определения составляющим информационной безопасности: идентификация и аутентификация (Identification Authentication), неотказуемость (Non-repudiation), подотчетность (Accountability)
4. Перечислите виды угроз информационной безопасности и дайте краткое их определение.
5. Проведите классификацию угроз ИБ по природе возникновения и по степени преднамеренности.
6. Проведите классификацию угроз ИБ по источнику угроз и положению источника угроз
7. Проведите классификацию угроз ИБ по степени зависимости от активности ИС и степени воздействия на ИС
8. Проведите классификацию угроз ИБ по этапам доступа пользователей к ресурсам и по способу доступа к ресурсам ИС.

Основы информационной безопасности. Часть 1: Виды угроз
https://habr.com/ru/company/vps_house/blog/343110/

9. Этапы развития информационной безопасности. Расскажите о развитии информационной безопасности до 1946 года
10. Этапы развития информационной безопасности. Расскажите о развитии информационной безопасности начиная с 1946 года

Лекция 4 по ИБ. Этапы развития информационной безопасности http://uskov.info/lektsii-po-informatsionnoj-bezopasnosti/lektsiya-4-po-ib-e-tapy-razvitiya-ib/

11. Защита информации от копирования. Расскажите об организационных, юридических и физических мерах.
12. Защита информации от копирования. Расскажите об аппаратных мерах защиты информации.
13. Защита информации от копирования. Расскажите о программных мерах защиты информации.
14. Что такое система защиты программы от копирования?
15. Политика и модели информационной безопасности.
16. Разграничение прав доступа. Идентификация и аутентификация пользователей. Объекты и субъекту доступа.
17. Дайте краткие характеристики подходов к определению прав доступа – избирательного и принудительного.
18. Дискреционная модель доступа. Матрица доступа. Элементы матрицы доступа. Листы возможностей и листы контроля доступа. Маркер доступа. Дескриптор защиты.

19. Мандатная модель доступа. Монитор обращения. Требования к мандатному механизму.
20. Мандатная модель доступа. Мандатный принцип контроля доступа
21. Мандатная модель доступа. Два правила доступа к защищённым файлам
22. Как организован контроль доступа в ОС Windows NT?
23. Как организован контроль доступа в ОС UNIX?
24. Достоинства и недостатки дискреционной и мандатной моделей.

Различают два основных подхода к определению прав доступа https://mylektsii.ru/7-27713.html

25. Вредоносные программы. Классификация. Способы защиты.
26. Криптографическая защита информации. Понятие криптологии, криптографии и криптоанализа. Для решений каких проблем безопасности применяются криптографические методы?
27. Перечислите способы обеспечения конфиденциальность информации между абонентами. Базовые методы преобразования информации в криптологии.
28. Наивная криптография. Алгоритмы, использовавшиеся на первом этапе развития криптографии.
29. Формальная криптология. Алгоритмы, использовавшиеся на втором этапе развития криптографии.
30. Криптоанализ . Методы Касицкого и Фридмана.
31. Научная криптология. Основы научной криптологии. Работы Шеннона.
32. Научная криптология. Абсолютно стойкие алгоритмы. Одноразовый блокнот Вернама.
33. Компьюторная криптография. Блочные шифры. Алгоритм DES.
34. Компьюторная криптография. Блочные шифры. Алгоритм ГОСТ 28147-89.
35. Компьюторная криптография. Алгоритм RSA.
36. Хэш-функции. Основные понятия и определения. Требования к хэш-функциям.
37. Хэш-функции. Метод Деления с остатком. Метод умножения. Универсальное хэширование.
38. Криптографические хэш-функции. Типы криптографических хэш-функций. Сравнение SHA и MD5.

Лекция 7: Криптографические хеш-функции. https://www.intuit.ru/studies/courses/691/547/lecture/12381?page=1

39. Электронная цифровая подпись: определение, юридическая сила, требования к ЭЦП, преимущества ЭЦП.
40. Электронная цифровая подпись. Принцип работы. Виды ЭЦП. Ключ и сертификат ЭЦП.
41. Электронная цифровая подпись. Алгоритмы в основе ЭЦП.
42. Что такое DoS-атака? Перечислите группы методов обнаружения DoS-атак. Перечислите меры противодействия DoS-атакам. Назовите причины, из-за которых может возникнуть DoS-условие
43. Что такое DDoS-атака? Назовите два типа DDoS атак Как классифицируются DDoS-атаки?
44. Что такое атаки на уровне протоколов? Что такое атаки на уровне приложений?
45. Что такое Флуд (англ. flood)? Какова основная цель использования флуда? Как защитится от флуда?

46. Как защититься от перегрузки аппаратных ресурсов? Что такое Storm?

47. Перечислите методы противодействия эксплуатации уязвимостей в софте.

48. Основные схемы подключения межсетевых экранов. Схемы защиты сети с использованием экранирующего маршрутизатора. Схемы с защищаемой закрытой и незащищаемой открытой подсетями.

49. Основные схемы подключения межсетевых экранов. Схемы с раздельной защитой, закрытой и открытой подсетей. Схемы единой защиты локальной сети.

50. Политика работы межсетевого экрана. Принцип «запрещено все, что явно не разрешено» и Принцип «разрешено все, что явно не запрещено»

51. Технология NAT/ Достоинства и недостатки NAT-технологии.

52. Классификация угроз, реализуемых по сети. Атаки в сетях на основе стека протоколов TCP/IP. Защита от sniffer'ов.

53. Спуфинг и антиспуфинг.

54. Преобразование адресов при использовании функции NAT. Три базовые концепции трансляции адресов. Четыре типа трансляции сетевых адресов.

55. Опишите, как работает межсетевой экран.

56. Технология персонального сетевого экранирования.

57. Распределенный межсетевой экран.

58. Функции посредничества межсетевого экрана. Выполнение функций посредничества межсетевым экраном.

59. Классификация межсетевых экранов по функционированию на уровнях модели OSI. Управляемые коммутаторы. Пакетные фильтры

60. Классификация межсетевых экранов по функционированию на уровнях модели OSI. Шлюзы сеансового уровня. Прикладные шлюзы, посредники прикладного уровня (Application Gateway).

61. Классификация межсетевых экранов по функционированию на уровнях модели OSI. Шлюзы экспертного уровня, инспекторы состояния (Stateful Inspection Firewall).