

- 1) Понятие управления (менеджмента).
- 2) Виды управления (менеджмента).
- 3) Принципы управления (менеджмента).
- 4) История развития управления (менеджмента).
- 5) Современные подходы в управлении (менеджменте).
- 6) Предприятие, как объект управления.
- 7) Управляющий (менеджер) в предприятия.
- 8) Внешняя и внутренняя среда предприятия.
- 9) Взаимодействие факторов окружающей среды предприятия.
- 10) Характеристика функций управления предприятием.
- 11) Понятие планирования и его виды.
- 12) Понятие стратегического планирования.
- 13) Понятие тактического планирования.
- 14) Понятие оперативного планирования.
- 15) Иерархический тип структур управления.
- 16) Линейная организационная структура.
- 17) Линейно-штабная организационная структура.
- 18) Дивизионная организационная структура.
- 19) Органический тип структур управления.
- 20) Бригадная (кросс-функциональная) структура управления.
- 21) Проектная структура управления.
- 22) Матричная (программно-целевая) структура управления.
- 23) Многомерная организационная структура.
- 24) Составляющие мотивации.
- 25) Критерии мотивации.
- 26) Теории мотивации.
- 27) Понятие и этапы контроля.
- 28) Виды и принципы контроля.
- 29) Технология и правила контроля.

- 30) Цели, задачи, предпосылки и направления организационной и управленческой работы в сфере информационной безопасности.
- 31) Структура управления информационной безопасностью.
- 32) Предпосылки развития государственного управления в сфере.
- 33) Общая методология и структура организационного обеспечения информационной безопасности на уровне государства.
- 34) Общая политика РФ в сфере информационной безопасности.
- 35) Предпосылки к управлению информационной безопасностью предприятия.
- 36) Структура управления информационной безопасностью предприятия.
- 37) Структура политики информационной безопасности и процесс ее разработки.
- 38) Политика информационной безопасности предприятия – верхний уровень.
- 39) Политика информационной безопасности предприятия – средний уровень.
- 40) Политика информационной безопасности предприятия – нижний уровень.
- 41) Внутриобъектовый режим; охрана помещений и территорий.
- 42) Физическая защита объектов.
- 43) Организация режима секретности.
- 44) Политика опубликования материалов в открытых источниках.
- 45) Политика управления паролями.
- 46) Политика установки и обновления версий программного обеспечения.
- 47) Политика приобретения информационных систем и их элементов.
- 48) Политика доступа сторонних пользователей (организаций).
- 49) Политика в отношении разработки программного обеспечения.

50) Политики использования отдельных универсальных информационных технологий.

51) Политика использования коммуникационных средств.

52) Политика использования мобильных аппаратных средств.

53) Департамент информационной безопасности.

54) Организационная структура и персонал департамента информационной безопасности.

55) Работа с персоналом предприятия.

56) Организация реагирования на чрезвычайные ситуации (инциденты).

57) Обнаружение атак и распознавание вторжений.

58) Локализация и устранение последствий на инцидент.

59) Идентификация нападающего.

60) Оценка и анализ процесса нападения и его обстоятельств.

61) Заключительные этапы процесса реагирования на инцидент.

62) Цели аудитов информационной безопасности, их классификации по типам.

63) Этапы аудита информационной безопасности.

64) Проверка состояния физической безопасности информационной инфраструктуры аудите информационной безопасности.

65) Инструментальная проверка защищенности при аудите информационной безопасности.

66) Анализ информации при аудите информационной безопасности.

67) Применение программных средств управления информационной безопасностью.

68) Программная поддержка политики безопасности.

69) Программная поддержка анализа рисков.

70) Программные средства, интегрируемые в информационную систему предприятия.

71) Рынок услуг по управлению информационной безопасностью.

- 72) Характеристики услуг управления информационной безопасностью.
- 73) Инфраструктура публичных ключей.
- 74) Основы методологии страхования информационных рисков.
- 75) Рынок страховых услуг.
- 76) Основы экономики информационной безопасности.
- 77) Анализ вложений в средства защиты информации.
- 78) Характеристика международных организаций в сфере управления информационной безопасностью.
- 79) Международный союз электросвязи.
- 80) Институт инженеров по электронике и электротехнике.
- 81) Ассоциация вычислительной техники.
- 82) Консорциум Всемирной Паутины.
- 83) Международная организация по стандартизации.
- 84) Характеристика специализированных международных организаций в сфере управления информационной безопасностью.
- 85) Координационный центр CERT CERTCC.
- 86) Исследовательская группа X-Force.
- 87) Характеристика специализированных международных объединений в сфере управления информационной безопасностью.
- 88) Альянс по смарт-картам – SCA.
- 89) Международная ассоциация компаний-производителей биометрического оборудования.
- 90) Методология управления информационной безопасностью поставщиками информационных систем.
- 91) Управление информационной безопасностью поставщиками информационных систем – Корпорация Microsoft.
- 92) Управление информационной безопасностью поставщиками информационных систем – Корпорация Cisco Systems.

Контрольные вопросы для проведения текущего контроля успеваемости по дисциплине –
Планирование и управление информационной безопасностью

93) Управление информационной безопасностью поставщиками информационных систем – Корпорация Cisco Systems.

94) Общая политика США в сфере управления информационной безопасностью.

95) Органы управления информационной безопасностью в США.

96) Федеральные программы и инициативы, поддерживаемые государством в США.