

Управление информационной безопасностью  
Контрольные вопросы для проведения текущего контроля по итогам освоения Раздела 2 –  
Теоретические аспекты планирования и управления информационной безопасностью  
предприятия

- 1) Цели, задачи, предпосылки и направления организационной и управленческой работы в сфере информационной безопасности.
- 2) Структура управления информационной безопасностью.
- 3) Предпосылки развития государственного управления в сфере.
- 4) Общая методология и структура организационного обеспечения информационной безопасности на уровне государства.
- 5) Общая политика РФ в сфере информационной безопасности.
- 6) Предпосылки к управлению информационной безопасностью предприятия.
- 7) Структура управления информационной безопасностью предприятия.
- 8) Структура политики информационной безопасности и процесс ее разработки.
- 9) Политика информационной безопасности предприятия – верхний уровень.
- 10) Политика информационной безопасности предприятия – средний уровень.
- 11) Политика информационной безопасности предприятия – нижний уровень.
- 12) Внутриобъектовый режим; охрана помещений и территорий.
- 13) Физическая защита объектов.
- 14) Организация режима секретности.
- 15) Политика опубликования материалов в открытых источниках.
- 16) Политика управления паролями.
- 17) Политика установки и обновления версий программного обеспечения.
- 18) Политика приобретения информационных систем и их элементов.
- 19) Политика доступа сторонних пользователей (организаций).
- 20) Политика в отношении разработки программного обеспечения.

Управление информационной безопасностью  
Контрольные вопросы для проведения текущего контроля по итогам освоения Раздела 2 –  
Теоретические аспекты планирования и управления информационной безопасностью  
предприятия

- 21) Политики использования отдельных универсальных информационных технологий.
- 22) Политика использования коммуникационных средств.
- 23) Политика использования мобильных аппаратных средств.
- 24) Департамент информационной безопасности.
- 25) Организационная структура и персонал департамента информационной безопасности.
- 26) Работа с персоналом предприятия.
- 27) Организация реагирования на чрезвычайные ситуации (инциденты).
- 28) Обнаружение атак и распознавание вторжений.
- 29) Локализация и устранение последствий на инцидент.
- 30) Идентификация нападающего.
- 31) Оценка и анализ процесса нападения и его обстоятельств.
- 32) Заключительные этапы процесса реагирования на инцидент.
- 33) Цели аудитов информационной безопасности, их классификации по типам.
- 34) Этапы аудита информационной безопасности.
- 35) Проверка состояния физической безопасности информационной инфраструктуры аудите информационной безопасности.
- 36) Инструментальная проверка защищенности при аудите информационной безопасности.
- 37) Анализ информации при аудите информационной безопасности.
- 38) Применение программных средств управления информационной безопасностью.
- 39) Программная поддержка политики безопасности.
- 40) Программная поддержка анализа рисков.

Управление информационной безопасностью  
Контрольные вопросы для проведения текущего контроля по итогам освоения Раздела 2 –  
Теоретические аспекты планирования и управления информационной безопасностью  
предприятия

- 41) Программные средства, интегрируемые в информационную систему предприятия.
- 42) Рынок услуг по управлению информационной безопасностью.
- 43) Характеристики услуг управления информационной безопасностью.
- 44) Инфраструктура публичных ключей.
- 45) Основы методологии страхования информационных рисков.
- 46) Рынок страховых услуг.
- 47) Основы экономики информационной безопасности.
- 48) Анализ вложений в средства защиты информации.