

Организационное и правовое обеспечение защиты информации
Контрольные вопросы для проведения текущего контроля по итогам освоения дисциплины

- 1) Структура и состав информационного законодательства.
- 2) Основные определения в области информационного права.
- 3) Классификация и виды информационных ресурсов.
- 4) Правовое регулирование информационного взаимодействия в компьютерных сетях.
- 5) Правовое обеспечение защиты государственной тайны.
- 6) Контроль и надзор за обеспечением защиты государственной тайны.
- 7) Правовая защита конфиденциальной информации.
- 8) Нормативно-правовое регулирование профессиональной тайны.
- 9) Нормативно-правовое регулирование служебной тайны.
- 10) Организационные меры по охране конфиденциальности информации.
- 11) Правовая основа системы лицензирования и сертификации в РФ.
- 12) Лицензирование деятельности по защите государственной тайны.
- 13) Сертификация средств защиты информации.
- 14) Лицензирование и сертификация в области защиты конфиденциальной информации.
- 15) Объекты интеллектуальной собственности.
- 16) Правовая охрана авторских и смежных прав.
- 17) Правовая охрана программ для ЭВМ и баз данных.
- 18) Технические средства защиты авторских прав.
- 19) Охрана типологии интегральных микросхем.
- 20) Классификация компьютерных преступлений
- 21) Криминалистические особенности расследования компьютерных преступлений.
- 22) Международные стандарты и соглашения в области безопасности информационных технологий.

Организационное и правовое обеспечение защиты информации
Контрольные вопросы для проведения текущего контроля по итогам освоения дисциплины

- 23) Направления, принципы и условия организационной защиты информации.
- 24) Подходы и требования к организации системы защиты информации.
- 25) Методы, силы и средства, используемые для организации защиты информации.
- 26) Средства и методы физической защиты объекта.
- 27) Структура системы физической защиты.
- 28) Процедурные меры обеспечения информационной безопасности.
- 29) Программно-технические методы обеспечения информационной безопасности.
- 30) Понятие режима секретности, его особенности и содержание.
- 31) Порядок работы с секретными документами и изделиями.
- 32) Допуск и доступ к информации, составляющей государственную тайну.
- 33) Допуск предприятий, учреждений и организаций к государственной тайне.
- 34) Технические каналы утечки компьютерной информации.
- 35) Защита информации от утечки по техническим каналам.