

- I. Угрозы Информационной безопасности и непрерывности бизнеса
 1. Какие задачи решает информационная безопасность?
 2. Что входит в понятие обеспечение непрерывности бизнеса?
 3. Дайте определение термину «угроза».
 4. Перечислите основные нормативно-правовые документы регулирующие область ИБ в РФ.
 5. Перечислите основные признаки безопасности информации?
 6. Перечислите основные категории угроз и приведите пример для каждой из них?
 7. Опишите основные этапы атаки?
 8. Каким образом строятся атаки основанные на социальной инженерии?
 9. Перечислите основные компоненты ботнета?
- II. Обработка рисков
 1. Дайте определение риска?
 2. Какие компоненты влияют на величину риска?
 3. Как работает количественный метод оценки риска?
 4. Каким образом производится подсчет стоимости актива?
 5. Каким образом считается ущерб от атаки?
 6. В чем заключаются недостатки количественного метода?
 7. Как используется качественный метод при анализе рисков?.
 8. В чем недостаток качественного метода?
 9. В чем преимущество качественного метода?.
 10. В чем заключается метод Дельфи?
 11. Что такое реестр рисков?
 12. Что такое политика ИБ?
 13. Перечислите методы работы с риском?
 14. Какая связь между политикой ИБ и реестром рисков
- III. Технологии Защиты
 1. Дайте определение аутентификации.
 2. Дайте определение авторизации.
 3. Перечислите основные технологии аутентификации.
 4. Перечислите основные протоколы аутентификации.
 5. В чем различие между SAML и OATH.
 6. В чем заключаются основные функции антивируса
 7. Перечислите основные методы обнаружения вирусов?
 8. В чем заключаются недостатки сигнатур?
 9. В чем заключаются недостатки поведенческого метода?

10. Перечислите основные виды межсетевых экранов
 11. Дайте определение межсетевого экрана
 12. Используются ли межсетевые экраны для защиты Ethernet ?
 13. Какие способы аутентификации используются для сети WiFi?
 14. Какие технологии используются для защиты пользовательских устройств ?
 15. Объясните принцип работы электронной подписи
- IV. Аудит и управление инцидентами
1. Перечислите основные стандарты используемые для проведения аудита ИБ ?
 2. Проводится ли аудит процедур работы с персоналом при аудите ИТ?
 3. Какие технологии используются для обеспечения непрерывности работы сервисов?
 4. Что такое SIEM ?
 5. Что такое системы DLP?
 6. Что означают аббревиатуры SaaS, IaaS, PaaS ?
 7. В чем различие “холодного” и “горячего” сайтов?
 8. Что представляет собой цифровая подпись ?
 9. Перечислите основные этапы работы с инцидентом ?
 10. В чем заключается роль аудитора ИБ?
 11. Какие документы позволяют судить о процессе разработки ПО в компании ?
 12. В чем различие между Waterfall и Agile подходами к разработке ПО.