Вопросы ОИБ 2018

Допуск – принятый отчет по практической работе (иметь при себе)
Порядок сдачи экзамена/зачета – устный ответ на билет (2 вопроса)

1. Теория защиты информации. Основные направления и определения. Категорирование информации.
2. Основные принципы обеспечения информационной безопасности в АС.
3. Угрозы безопасности информации. Классификация. Источники угроз. Предпосылки появления угроз.
4. Риски информационной безопасности. Количественная и качественная оценка рисков. Управление рисками.
5. Каналы несанкционированного доступа. Классификация.
6. Классы задач защиты информации. Функции системы защиты информации
7. Состояния системы защиты информации
8. Стратегии защиты информации
9. Способы и средства защиты информации
10. Система защиты информации с полным перекрытием. «Абсолютная» система защиты
11. Вредоносное ПО. Правовые аспекты. Стандартные методы заражения
12. Вредоносное ПО. Вирусы, черви, троянские программы, рекламное ПО
13. Вредоносное ПО. Шпионское ПО, программы-вымогатели, боты, руткиты
14. Особенности ИБ в компьютерных сетях. Модель OSI. Стек TCP/IP
15. Специфика средств защиты в компьютерных сетях, сетевые модели передачи данных, принципы организации обмена данными в вычислительных сетях
16. Классификация удаленных угроз в вычислительных сетях
17. Криптография, основные термины
18. Криптография: симметричные, асимметричные методы шифрования, атаки на алгоритмы
19. Стеганография, основные определения, цифровая стеганография
20. Области встраивания в цифровые изображения, стегоанализ, признаки в областях встраивания, на основе которых производится стегоанализ
21. Целенаправленные атаки, пять этапов проникновения. Индикаторы взлома корпоративных сетей
22. Комплексная система нейтрализации целенаправленных атак
23. Социальная инженерия, человеческий фактор, умышленные/неумышленные действия, обратная социальная инженерия
24. Техники социальной инженерии. Основные меры предостережения
25. Фишинг, спирфишинг, ransomware
26. KillChain. Стадии, варианты модификации
27. Методы борьбы с фишингом на предприятиях, предотвращение последующих атак. Примеры.
28. Противодействие киберприступности, стратегии для защиты и приватности, повышение устойчивости критических систем
29. История развития беспроводных сетей. Особенности функционирования с точки зрения ИБ. (Отличия проводных и беспроводных технологий передачи данных)
30. Основные риски беспроводной связи, угрозы, атаки, утечки информации из проводной сети
31. Руководящий документ «Классификация автоматизированных систем и требований по защите информации".
32. Стандарт США «Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США". Основные положения
33. Регуляторы в области защиты информации