Вопросы к зачету
по дисциплине «Гуманитарные аспекты информационной безопасности»
для специальности «Компьютерная безопасность»
составил: к.т.н., доцент, Иванцов Андрей Михайлович

4 семестр

Примерный перечень вопросов к зачету:

1. Гуманитарная сущность безопасности. Основные нормативно-правовые акты России по вопросам безопасности.
2. Гуманитарная сущность информации. Технократический и гуманитарный подходы к информации.
3. Гуманитарная сущность информационной безопасности.
4. Место и роль проблем информационной безопасности в становлении современного информационного общества.
5. Системный кризис цивилизации и его гуманитарные причины.
6. Нравственные приоритеты молодого поколения и будущее России как один из аспектов проблемы информационной безопасности.
7. Стадии формирования информационной безопасности (ИБ). Институционализация отрасли ИБ.
8. Стадии формирования информационной безопасности (ИБ). Профессионализация отрасли ИБ.
9. Стадии формирования информационной безопасности (ИБ). Технологизация отрасли ИБ.
10. Стадии формирования информационной безопасности (ИБ). Социализация отрасли ИБ.
11. Формирование информационной культуры общества. Этика в сфере информационных технологий.
12. Основные элементы глобальная культуры кибербезопасности.
13. Всеобуч в области культуры информационной безопасности.
14. Международные и отечественные стандарты информационной безопасности.
15. Система управления информационной безопасности организации.
16. Основные функции и компоненты системы управления информационной безопасностью организации.
17. Область действия системы управления информационной безопасностью организации.
18. Документальное обеспечение системы управления информационной безопасностью организации.
19. Использование процессного подхода для разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения системы управления информационной безопасностью организации.
20. Основные этапы создания СУИБ (инвентаризация и категорирование активов; оценка защищенности информационной системы; оценка и обработка информационных рисков; контроль выполнения и эффективности выбранных мер).
21. Основные понятия управления рисками. Термины и определения.
22. Основные этапы управления рисками (выбор методологии оценки рисков; идентификация активов; анализ угроз и их последствий; выявление уязвимых мест в защите; оценка рисков; выбор защитных мер; реализация и проверка выбранных мер; оценка остаточного риска).
23. Нормативная база управления инцидентами информационной безопасности (ИБ). Понятие события и инцидента ИБ. Цели и задачи управления инцидентами ИБ.
24. Система управления инцидентами ИБ.
25. Этапы процесса управления инцидентами ИБ.
26. Политика управления инцидентами ИБ.
27. Обеспечение осведомленности и обучение в области инцидентов ИБ.

28. Политика информационной безопасности (ПИБ) предприятия. Содержание ПИБ.
29. Область применения Политики информационной безопасности (ПИБ). Понятие ПИБ «в широком» и «в узком» смыслах. «Частные» ПИБ.
30. Обязанности руководителя и сотрудников отдела информационной безопасности по предупреждению, реагированию и ликвидации последствий нарушений безопасности.
31. Требования безопасности, предъявляемые к пользователям информационной системы.
32. Основные мероприятия, формальные процедуры и другие технологические процессы по обеспечению информационной безопасности.
33. Система управления непрерывностью бизнеса (СУНБ).
34. Внедрение управления непрерывностью бизнеса в культуру организации. Программа непрерывного образования и информирования об управлении непрерывностью бизнеса.
35. Общая характеристика планов управления инцидентами, обеспечения непрерывности бизнеса и восстановления бизнеса. Примерное содержание плана обеспечения непрерывности бизнеса.
36. Методология проверки и оценки состояния информационной безопасности.
37. Аудиты информационной безопасности на соответствие требованиям нормативных документов. Этапы проведения аудита ИБ.
38. Общие требования к системе защиты информации. Требования к подсистемам системы защиты информации.