Выписка из программы ГИА

Государственный междисциплинарный экзамен
по направлению подготовки 10.03.01 «Информационная безопасность»
(уровень – академический бакалавриат)

В билет государственного междисциплинарного экзамена входят два вопроса. Первый вопрос – из раздела 1 программы (для всего направления подготовки); второй вопрос – из раздела 2 (для профиля Безопасность автоматизированных систем) программы. В одном билете должны быть вопросы из разных модулей (дисциплин) учебного плана.

Государственный экзамен предусматривает оценивание уровня овладения выпускниками компетенций, установленных ФГОС ВО и дополнительных компетенций, установленных ООП ВО.

Контрольные вопросы программы государственного междисциплинарного экзамена по направлению подготовки 10.03.01 «Информационная безопасность»
(в редакции 2024/25 уч. гг.)

Раздел 1. Вопросы по направлению подготовки

1. Понятие и сущность информационной безопасности современного общества. Доктрина информационной безопасности. Государственная система защиты информации.
2. Принципы, критерии и условия отнесения информации к защищаемой. Классификация конфиденциальной информации по видам тайн.
3. Объекты защиты информации, их классификация и особенности.
4. Понятие угрозы нарушения информационной безопасности; виды угроз. Источники угроз нарушения целостности, доступности и конфиденциальности информации.
5. Каналы и методы несанкционированного доступа к конфиденциальной информации.
6. Понятие риска нарушения информационной безопасности. Методы анализа и управление информационными рисками.
7. Сущность моделирования информационных процессов и систем. Разработка моделей комплексной системы защиты информации.
8. Сущность, задачи, принципы построения и функционирования комплексной системы защиты информации. ТЭО проектов КСЗИ.
9. Лицензирование деятельности предприятий для проведения работ, связанных с использованием сведений, составляющих государственную тайну.
10. Организационные требования к режимным помещениям. Порядок сдачи и приема режимных помещений под охрану.

11. Виды и назначение технических средств охраны объектов.

12. Организация охраны объекта информатизации. Внутриобъектовый и пропускной режимы.

13. Понятие и сущность государственной тайны Особенности правовой защиты государственной тайны.

14. Понятие и сущность служебной, коммерческой и профессиональной тайны. Особенности правовой защиты служебной, коммерческой и профессиональной тайны.

15. Требования нормативных документов по защите персональных данных. Организация защиты персональных данных на предприятии.

16. Общие положения о допуске граждан к государственной тайне. Порядок оформления допуска.

17. Порядок доступа персонала и иных лиц к конфиденциальной информации.

18. Организация работы по засекречиванию и рассекречиванию сведений, составляющих государственную тайну и другой конфиденциальной информации.

19. Виды и состав стандартов и нормативных документов по информационной безопасности.

20. Аттестационные испытания, аттестация объектов информатизации.

21. Акустические (воздушные и вибрационные) каналы утечки информации. Способы противодействия.

22. Визуально-оптические каналы утечки информации. Способы противодействия.

23. Радиоэлектронные каналы утечки информации. Способы противодействия

24. Каналы утечки информации из технических систем и средств передачи, обработки, хранения и отображения информации. Способы противодействия.

25. Назначение, состав и технические характеристики закладочных устройств. Демаскирующие признаки закладочных устройств.

26. Базовые сервисы информационной безопасности компьютерных систем.

27. Разграничение доступа в операционных системах. Штатные средства идентификации/аутентификации субъектов доступа.

28. Криптосистемы с секретным и открытым ключом. Виды атак на них.

29. Сущность, назначение и применение электронной подписи. Схемы электронной подписи. Удостоверяющий центр.

30. Понятия базы данных, системы базы данных, банка данных, модели «сущность-связь».

31. Элементы системы управления базами данных. Схема базы данных.

32. Реляционная модель базы данных и нормализация

33. Многопользовательские базы данных, транзакции, виды транзакций, блокировка ресурсов.

34. Особенности правовой защиты объектов интеллектуальной собственности.

35. Основные современные формы информационной войны.

Раздел 2. Вопросы по профилю «Безопасность автоматизированных систем»

1. Сущность понятий «защита информации», «безопасность информации», «информационная безопасность».
2. Принципы, цели и теоретические основы защиты информации. Классификация видов, методов и средств защиты информации.
3. Источники, виды и способы дестабилизирующих воздействий на информацию.
4. Классификация носителей информации и особенности защиты зафиксированной на них информации.
5. Сущность и основные этапы организационного проектирования комплексной системы защиты информации.
6. Принципы, сущность и методы управления информационной безопасностью объекта.
7. Организационная защита информации в процессе издательской, рекламной и выставочной деятельности.
8. Организационная защита информации при проведении переговоров (совещаний) по конфиденциальным вопросам.
9. Организационная защита конфиденциальных изделий в процессе их изготовления, хранения и транспортировки.
10. Жизненный цикл подсистем защиты информации
11. Основные принципы разведки. Классификация технической разведки. Условия осуществления разведывательного контакта.
12. Системы электронного документооборота. Обеспечение безопасности электронного документооборота.
13. Политики информационной безопасности.
14. Классификация, назначение и основные характеристики средств обнаружения закладочных устройств.
15. Защита информации техническими способами и средствами.
16. Методы и средства противодействия наблюдению в оптическом и инфракрасном диапазонах.
17. Методы и средства защиты речевой информации.
18. Способы и средства предотвращения утечки информации через побочные излучения и наводки.
19. Активные и пассивные методы и средства защиты информации от утечки по радиоэлектронному каналу.
20. Криптосистемы с открытым ключом RSA и Эль-Гамаля.

21. Системы обнаружения вторжений в информационные системы. Классы защиты.

22. Система открытого распределения ключей Диффи-Хэллмана.

23. Виды атак на информационные системы. Методы обнаружения компьютерных атак.

24. Программные и программно-аппаратные средства защиты информации.

25. Понятие об администрировании систем информационной безопасности.

26. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.

27. Базовые этапы управления инцидентами информационной безопасности.

28. Средства обеспечения безопасности VPN. Классификация сетей VPN.

29. Протоколы формирования защищённых каналов на канальном и сеансовом уровнях модели OSI.

30. Архитектура стека протоколов IPSec