Вопросы к зачету по дисциплине информационная безопасность

1. Дайте определение информационной безопасности (ИБ). В чем разница между понятиями «защита информации» и «обеспечение ИБ»?
2. Чем риски ИБ отличаются от непосредственных угроз? Назовите три основные группы угроз.
3. Каковы основные национальные интересы РФ в информационной сфере согласно Доктрине информационной безопасности? Как в Стратегии национальной безопасности отражена роль пространственных данных (топографо-геодезическая информация)?
4. Раскройте значение терминов: лицензирование деятельности, сертификация СЗИ) аттестация объектов информатизации. Какие органы власти регулируют эти процессы?
5. Что относится к персональным данным? Каковы особенности обработки геолокационных данных с точки зрения 152-ФЗ?
6. Дайте определение коммерческой тайны. Могут ли цифровые карты местности и данные ДЗЗ)высокой детализации являться коммерческой или государственной тайной?
7. Перечислите виды юридической ответственности. Приведите примеры составов преступлений из УК РФ.
8. Какие задачи решает криптография? Какими средствами достигается неотказуемость от авторства?
9. В чем разница между симметричной и асимметричной криптографией? Приведите примеры алгоритмов.
10. Дайте определение криптографического протокола. Назовите основные свойства протокола.
11. Что такое криптографическая хэш-функция? Какими свойствами она обладает? Где применяется хэширование?
12. В чем разница между идентификацией и аутентификацией? Назовите три фактора аутентификации.
13. Раскройте понятия «дискреционный», «мандатный» и «ролевой» (RBAC) методы разграничения доступа. Какой метод наиболее применим для разграничения доступа к слоям в корпоративной ГИС?
14. Опишите модель нарушителя для автоматизированной системы (АС). По каким признакам классифицируют нарушителей?
15. Перечислите программно-аппаратные средства защиты от несанкционированного доступа. Что такое «доверенная загрузка» и межсетевые экраны?
16. Дайте определение технического канала утечки информации. На какие группы делятся ТКУ?
17. Что такое ПЭМИН? Какие меры защиты применяются для снижения риска перехвата информации по данному каналу?
18. Назовите классификацию вредоносного ПО. В чем разница между сигнатурным и эвристическим методами обнаружения угроз?
19. В чем разница между активной и пассивной антивирусной защитой? Приведите примеры активных методов.
20. Что такое антивирусная политика безопасности? Какие ключевые правила она включает?
21. В чем разница между комплексным и системным подходом к защите информации? Почему для ГИС-проектов важен именно системный подход?
22. Раскройте суть процессного подхода в управлении ИБ. Какую роль играет управление ИБ в структуре организации?
23. Приведите примеры организационных мер защиты. Почему человеческий фактор считается самым слабым звеном в ИБ?

24. Каковы особенности обеспечения безопасности при передаче данных по сетям общего пользования? Что такое VPN и как он обеспечивает защиту?
25. Перечислите основные классы средств защиты сетей: межсетевые экраны, системы обнаружения вторжений, прокси-серверы, средства анализа трафика.
26. Назовите основные типы сетевых атак. Какой тип угроз наиболее опасен при передаче геоданных по открытым каналам?
27. Что такое целостность данных? Перечислите типы ограничений целостности в реляционной модели. Как эти ограничения применимы к атрибутивной информации в ГИС?
28. В чем специфика защиты информации в государственных информационных системах (ГИС), содержащих пространственные данные?
29. Назовите основные стадии проектирования автоматизированных систем в защищенном исполнении.
30. Что такое Модель угроз безопасности информации? Для чего предназначен Банк данных угроз ФСТЭК России? Как используется этот банк данных при построении модели угроз для конкретной организации?
31. По каким критериям классифицируются государственные информационные системы и информационные системы персональных данных для определения уровня защищенности?
32. В чем суть множественной классификации систем? Приведите пример системы, которая может одновременно относиться к разным классам по разным признакам.
33. Какие угрозы информационной безопасности возникают при проведении полевых геодезических работ? Предложите меры защиты.
34. Опишите угрозы для систем, использующих ГНСС (GPS/ГЛОНАСС): спуфинг и глушение. Как эти угрозы могут повлиять на работу систем мониторинга транспорта или геодезических сетей?
35. Как можно использовать методы стеганографии применительно к цифровым растровым изображениям или векторным слоям?
36. Какие специфические уязвимости характерны для веб-приложений? Чем опасна неправильная настройка CORS для геосервисов?
37. Почему метаданные цифровых карт являются объектом защиты информации с точки зрения целостности и аутентичности?
38. В связи с уходом зарубежных вендоров (ESRI, Autodesk), какие риски информационной безопасности возникли для российских организаций, использующих проприетарное геопрограммное обеспечение? Как снизить эти риски?
39. Какие угрозы существуют при использовании дронов для сбора геоданных? Каковы методы защиты каналов управления и телеметрии?
40. В чем заключаются риски при размещении пространственных данных в публичных облачных хранилищах (SaaS, IaaS)? Как обеспечивается разграничение доступа к «облачной» ГИС?