Российский государственный университет нефти и газа
(национальный исследовательский университет)
имени И.М. Губкина

Утверждена проректором по науч-
ной и международной работе
проф. А.Ф. Максименко
14 апреля 2022 года

П Р О Г Р А М М А

вступительного испытания по научной специальности
2.3.6. «Методы и системы защиты информации, информационная безопасность»
для поступающих в аспирантуру РГУ нефти и газа (НИУ) имени И.М. Губкина
в 2022/2023 уч. году

Москва 2022

Введение

Программа вступительного испытания по научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность» разработана на основании требований, установленных паспортом специальности.

Основы обеспечения информационной безопасности

1. Основные термины и определения в области информационной безопасности.
2. Информационная безопасность и защита информации.
3. Понятие угрозы безопасности информации. Классификация угроз.
4. Основные аспекты информационной безопасности: конфиденциальность, целостность, доступность.
5. Понятие национальной безопасности; виды безопасности; информационная безопасность в системе национальной безопасности Российской Федерации.
6. Классификация информации (К, С, СС, ОВ). Перечень информации, которой не может быть присвоен статус ограниченного распространения.
7. Различные категории информации, подлежащие защите (государственная тайна, коммерческая тайна, персональные данные…).
8. Доктрина информационной безопасности Российской Федерации.
9. Органы государственной власти, регулирующие деятельность в области обеспечения информационной безопасности.
10. Структура нормативной правовой базы Российской Федерации в области обеспечения информационной безопасности.
11. Деятельность государственных органов РФ, контролирующих деятельность в области информационной безопасности, их роль в формировании и актуализации государственной системы защиты информации в РФ.
12. Управление информационной безопасностью. Процессный подход.
13. Понятие системы управления информационной безопасностью (СУИБ).
14. Стандарты серии ISO 27000.
15. Понятие риска информационной безопасности. Анализ рисков.
16. Основные процессы СУИБ. Документирование СУИБ.
17. Технические каналы утечки информации.
18. Защита информации от утечки по техническим каналам.
19. Специальные исследования технических средств на наличие технических каналов утечки информации.

Криптографические методы защиты информации

20. Криптология. Понятия криптографии, криптоанализа, стеганографии. Основные термины и определения: шифрование, расшифрование, дешифрование.
21. Симметричные криптосистемы. Принципы работы и основные понятия. Пример реализации.
22. Асимметричные криптосистемы. Принципы работы и основные понятия. Пример реализации.
23. Потоковые и блочные шифры.
24. Цифровая подпись. Протокол цифровой подписи на симметричном шифре.
25. Цифровая подпись. Протокол цифровой подписи на асимметричных криптоалгоритмах.

26. Алгоритмы блочного шифрования AES, DES, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015. Слабые ключи итеративных симметричных блочных шифров.
27. Протоколы аутентификации. Базовые конструкции протоколов аутентификации. Аутентификация по паролю (списки паролей, протокол Лампорта). Аутентификация «запрос – ответ» (ISO/IEC 9798). Принцип аутентификации, основанный на нулевом разглашении (протоколы Фиата – Шамира, Файге – Фиата – Шамира).

Основы численного моделирования и оптимизации

28. Алгоритмы численного решения систем линейных алгебраических уравнений. Проблема обусловленности.
29. Алгоритмы численного решения нелинейных уравнений и систем нелинейных уравнений.
30. Вычислительные методы восстановления значений функций.
31. Алгоритмы численного решения дифференциальных уравнений.
32. Алгоритмы численного решения задач безусловной оптимизации.
33. Алгоритмы численного решения задач условной оптимизации.
34. Постановка задачи многокритериальной оптимизации и её проблемы.
35. Общая задача линейного программирования; симплекс-метод.
36. Постановка и решение задач целочисленного линейного программирования. Алгоритмы "ветвей и границ".
37. Задачи выпуклого программирования. Метод неопределённых множителей Лагранжа.
38. Транспортная задача.
39. Метод динамического программирования и его применение в задачах распределения ресурсов.

Случайные процессы и статистический анализ

40. Имитационное моделирование. Методы генерации случайных величин.
41. Случайные процессы. Марковские случайные процессы. Цепи Маркова с дискретным и непрерывным временем, метод динамики средних.
42. Теория массового обслуживания. Системы массового обслуживания (разомкнутые, замкнутые). Определение характеристик типовых СМО и их эффективности.
43. Регрессионный анализ.
44. Корреляционный анализ.
45. Задачи классификации; дискриминантный и кластерный анализ.

Модели и методы принятия решений

46. Постановка задач принятия решений. Классификация, этапы решения. Экспертные процедуры. Экспертные оценки и обработка результатов экспертизы.
47. Принятие решений в условиях неопределённости. Нечёткие системы и методы определения функций принадлежности.
48. Задачи математического программирования при нечётких исходных условиях. Задача выбора вариантов проектов.

49. Игровые модели принятия решений. Биматричные игры: равновесие по Нэшу и Парето. Игры с природой (теория статистических решений). Критерии Сэвиджа, Вальда, Гурвица.

Методы и средства обработки информации в современных информационных системах

50. Этапы проектирования базы данных. Процесс нормализации отношений в реляционной базе данных. Хранилища данных. Оперативная аналитическая обработка (OLAP).
51. Понятия "данные", "информация", "знания" в приложении к Data Mining. Классификация методов Data mining.
52. Основные компоненты объектно-ориентированного подхода. Объекты и классы с точки зрения проектирования и программирования.
53. Обработка ошибок в современном программном обеспечении. Обработка исключительных ситуаций, структурная обработка аппаратных исключений.
54. Структурные и функциональные методы тестирования программ. Методы оценки надёжности программных комплексов.
55. Принципы построения современных операционных систем. Архитектура памяти, процессы, многозадачность. Основные ситуации, требующие синхронизации.
56. Основные принципы построения систем реального времени. Области применения, требования, особенности разработки.
57. Защита информации в информационных системах: основные понятия, этапы построения и принципы проектирования систем защиты.
58. Криптографические методы защиты информации. Симметричные и асимметричные алгоритмы шифрования, цифровая подпись.
59. Средства обеспечения сетевой защиты: межсетевые экраны, системы обнаружения атак и анализа защищённости, виртуальные защищённые сети.
60. Технологии систем хранения данных: основные задачи, подходы к организации.

Программно-аппаратные средства обеспечения информационной безопасности

61. Классификация АС по требованиям безопасности информации (РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»).
62. Установление подлинности пользователя. Парольные, физические и биометрические методы подтверждения подлинности. Понятие факторность методов подтверждения подлинности. Сравнение методов по степени обеспечения уровня информационной безопасности.
63. Этапы развития криптографической подсистемы. Цифровой сертификат. ЭЦП. Технология «цифрового конверта».
64. Основные принципы создания системы защиты информации от несанкционированного доступа (принцип персональной ответственности, принцип чистоты повторно используемых ресурсов, монитор обращений).
65. Основные принципы создания системы защиты информации от несанкционированного доступа (принцип достаточной глубины контроля доступа, принцип разграничения потоков информации, монитор обращений).

66. Классификация и краткая характеристика средств обеспечения информационной безопасности в компьютерных сетях. Системы анализа защищенности. Организация и использование средств доказательной регистрации событий (аудита).
67. Межсетевые экраны. Фильтрация трафика. Системы обнаружения и предотвращения вторжений (IDS/IPS). SIEM-системы.

Литература

1. Антонов А.В., Никулин М.С. Статистические модели в теории надежности. М.: Абрис: 2012.
2. Бессмертный И.А. Искусственный интеллект: Учебное пособие. - СПб: СПбГУ ИТМО, 2010. - 132 с.
3. Большаков А.А., Каримов Р.Н. Методы обработки многомерных данных и временных рядов. Серия: Специальность. Для высших учебных заведений. Издательство: Горячая Линия - Телеком, 2007 г
4. Буч Г., Максимчук Р., Энгл М., Янг Б., Коналлен Дж., Хьюстон К. Объектно-ориентированный анализ и проектирование с примерами приложений. Вильямс, 2010 г.
5. Васильев Ф.П. Методы оптимизации. Книга 1. / МЦНМО, М., 2011, 620 с.
6. Васильев Ф.П. Методы оптимизации. Книга 2. / МЦНМО, М., 2011, 432 с.
7. Вержбицкий В.М. Численные методы (линейная алгебра и нелинейные уравнения): Учеб. пособие для вузов. – М.: Оникс 21 век, 2005 г.
8. Вержбицкий В.М. Численные методы (математический анализ и дифференциальные уравнения): Учеб. пособие для вузов. – М.: М.: Оникс 21 век, 2005 г.
9. Гагарина Л.Г., Киселев Д.В., Федотова Е.Л. Разработка и эксплуатация автоматизированных информационных систем. – М.: ИД «ФОРУМ»-ИНФРА-М, 2009. – 383с.
10. Гнеденко Б.В, Коваленко И.Н. Введение в теорию массового обслуживания. Издательство: ЛКИ, 2007 г.
11. Гордеев А.В. Операционные системы : учебник для вузов / А. В. Гордеев. - 2-е изд. - СПб. : Питер, 2009. - 416 с.
12. Григорьев Л.И., Тупысев А.М., Санжаров В.В. Интеллектуальный анализ данных; методы и примеры использования в нефтегазовой отрасли. Учебное пособие. М.: РГУ нефти и газа имени И.М. Губкина, 2015 - 98 с.
13. Григорьев Л.И., Кершенбаум В.Я., Костогрызов А.И. Системные основы управления конкурентоспособностью в нефтегазовом комплексе. М.: Изд-во НИНГ 2010 - 374с.
14. Дейтел П.Дж., Дейтел Х.М., Чофнес Д.Р. Операционные системы. Распределенные системы, сети, безопасность 2011 г., 704 с
15. Древс Ю.Г. Системы реального времени: технические и программные средства: Учебное пособие. М.: МИФИ, 2010. 320 с.
16. Илюшечкин В.М. Основы использования и проектирования баз данных. -М.: Юрайт, 2010. -214 с.

17. Каштанов В.А., Медведев А.И. Теория надежности сложных систем. Учебное пособие Москва: Физматлит, 2010.- 608 с
18. Клейменов С.А. Информационная безопасность. Издание 5. ACADEMIA, 2010 г.
19. Корпоративные информационные системы управления: учебник / под ред. проф. Н.М. Абдикеева, доц. О.В. Китовой. – М.: ИНФРМА-М, 2012. – 464 с
20. Кузнецова Л.В., Леонов Д.Г. Методы и средства защиты информации: Курс лекций. МАКС Пресс, 2010.
21. Малинецкий Г.Г. Математические основы синергетики. Хаос, структуры, вычислительный эксперимент. Учебное пособие Изд.6-е. - М.: Издательство ЛКИ, 2012.- 312с. (Синергетика: от прошлого к будущему.).
22. Невежин В.П. Исследование операций и принятие решений в экономике / В. П. Невежин, С. И. Кружилов, Ю. В. Невежин, М. Изд-во Форум, 2012, 400 стр.
23. Олифер В.Г., Олифер Н.А. «Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов» 4-е изд. - СПб.: Питер, 2010. – 944 с.
24. Олифер В.Г., Олифер Н.А. «Сетевые операционные системы» – СПб.: Питер, 2009. – 672 с.
25. Редько В. Эволюция, нейронные сети, интеллект. Модели и концепция эволюционной кибернетики. М.: УРСС 2013.
26. Рябинин И. А. Надежность и безопасность структурно-сложных систем. СПб.: Издательство Санкт-Петербургского университета, 2007 г., 278 с.
27. Советов Б.Я., Яковлев С.А. Моделирование систем 7-е изд. М: Изд. Юрайт, 2012.
28. Степин Ю.П., Трахтенгерц Э.А. Компьютерная поддержка управления нефтегазовыми технологическими процессами и производствами. Методы и алгоритмы формирования управленческих решений. М.: РГУ нефти и газа им. И.М.Губкина, 2007. - 382 с.
29. Фарли М. Сети хранения данных. Изд. 2-е. М.: Издательство Лори, 2004 г.-576с.
30. Харари Ф. Теория графов : пер. с англ. - 4-е изд. - М. : Книжный дом «ЛИБРОКОМ», 2009. - 296 с.
31. Ясницкий Л.Н. Введение в искусственный интеллект: Учебное пособие для вузов Изд. 2-е, испр. – М.: Академия, 2008 г. – 176 с.
32. Малюк А.А. [и др.] Введение в информационную безопасность. – М.: «Горячая линия – Телеком», 2011. – 290 с. 9.
33. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2004. – 280 с. 10.
34. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. – М.: Горячая линия – Телеком, 2001. – 148 с
35. Алферов А.П. Основы криптографии. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Учебное пособие. – Москва : Гелиос АРВ, 2005. – 480 с.
36. Мао В. Современная криптография: теория и практика.– Москва: Издательский дом Вильямс, 2005. – 768 стр.
37. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 352 с.