УТВЕРЖДАЮ
И.о. проректора по научной работе,

_____К.В. Дукельский

«_31_» _марта_ 2015 г.

ПРОГРАММА ВСТУПИТЕЛЬНОГО ЭКЗАМЕНА ПО ПРОФИЛЮ 05.13.19 - МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1. Основы информационной безопасности

Основные понятия и принципы теории информационной безопасности.

Угрозы информационной безопасности, их анализ.

Виды информации, методы и средства обеспечения информационной безопасности.

Методы нарушения конфиденциальности, целостности и доступности информации.

Основы комплексного обеспечения информационной безопасности.

Модели, стратегии и системы обеспечения информационной безопасности.

Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.

Лицензирование и сертификация в области защиты информации.

Правовые основы защиты информации с использованием технических средств.

Защиты интеллектуальной собственности.

Основы законодательства в области защиты информации.

2. Избранные разделы математики

Методы решения систем линейных уравнений.

Методы интерполяции.

Методы численного интегрирования.

Методы численного решения дифференциальных уравнений.

Численные методы нахождения экстремумов функций.

Элементы комбинаторики: перестановки, выборки, сочетания и размещения без повторений.

Сочетания и размещения с повторениями, биномиальные коэффициенты, их свойства. Элементы теории графов: определение графа, способы представления.

Изоморфизм графов, элементы графов, валентность, маршруты, цепи, циклы.

Связность графов, подграфы, виды графов (тривиальные и полные; двудольные; планарные; направленные орграфы и сети) и операции над ними.

Алгебра логики, формулы алгебры логики, высказывания и операции, построение формул.

Булевы функции и формулы, функции алгебры логики, способы представления БФ, нормальные формы.

Карты Карно, минимизация БФ с помощью карт Карно.

Теоремы сложения и умножения вероятностей.

Формула полной вероятности Байеса.

Схема Бернулли, приближенные вычисления в схеме Бернулли.

Случайные величины, математическое ожидание и дисперсия.

Основные законы распределения случайной величины.

Многомерные случайные величины.

Центральная предельная теорема.

Цепи Маркова.

Задача о линейном программировании.

Система массового обслуживания без очереди.

Система массового обслуживания с очередью.

Марковские процессы с дискретным временем, матрицы перехода дискретной цепи Маркова, предельные вероятности.

Метод Монте-Карло. Основные определения и понятия.

Генерирование значений дискретных случайных величин.

Генерирование траекторий случайных процессов.

3. Вычислительная техника и программирование

Архитектура современных ЭВМ, принципы работы отдельных компонент.

Языки программирования высокого и низкого уровня, компиляторы и интерпретаторы.

Технология объектно-ориентированного программирования.

Операционные системы: функции ядра, функции защиты информации, основные типы ОС.

Локальные и глобальные вычислительные сети, типовые конфигурации, маршрутизация.

Основные протоколы обмена данными в вычислительных сетях, их информационная безопасность.

Системы управления базами данных, реляционная, иерархическая и сетевая модели, распределенные БД, защита информации в БД.

Теория сложности алгоритмов, классы сложности.

Деревья и графы, их представление в ЭВМ, обходы графов.

Алгоритмы на графах, выделение компонент связности.

Кратчайшие пути в графе, минимальный остов графа.

Деревья поиска и их применение.

Задача сортировки и основные алгоритмы сортировки.

Поиск информации методом хеширования.

Методы и средства привязки программ к аппаратному окружению и физическим носителям.

Методы и средства хранения ключевой информации в ЭВМ.

Защиты программ от изучения, защита от изменения и контроль целостности.

Защита от разрушающих программных воздействий.

4. Основы криптографии

История криптографии и ее основные достижения.

Шифры замены и перестановки, их свойства, композиции шифров.

Криптостойкость шифров, основные требования к шифрам.

Теоретическая стойкость шифров, совершенные и идеальные шифры.

Блоковые шифры.

Потоковые шифры.

Криптографические хеш-функции, их свойства и использование в криптографии.

Методы получения случайных последовательностей, их использование в криптографии.

Методы получения псевдослучайных последовательностей, их использование в криптографии.

Системы шифрования с открытыми ключами.

Криптографические протоколы.

Протоколы распределения ключей.

Протоколы идентификации.

Парольные системы разграничения доступа.

Цифровая подпись.

Стойкость систем с открытыми ключами.

5. Технические средства и методы защиты информации

Структура, классификация и основные характеристики технических каналов утечки информации.

Побочные электромагнитные излучения и наводки.

Классификация средств технической разведки, их возможности.

Концепция и методы инженерно-технической защиты информации.

Методы скрытия речевой информации в каналах связи.

Методы обнаружения и локализации закладных устройств.

Методы подавления опасных сигналов акустоэлектрических преобразователей.

Методы подавления информативных сигналов в цепях заземления и электропитания.

Виды контроля эффективности защиты информации.

Методы расчета и инструментального контроля показателей защиты информации.

Литература

1. Андерсон Дж. А. Дискретная математика и комбинаторика: Пер. с англ. - М.: Издат. дом «Вильямс», 2003 г.

2. Ахо А., Хопкрофт Дж., Ульман Д. Построение и анализ вычислительных алгоритмов.

3. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учеб. курс. - М.: Горячая линия-телеком, 2002 г. - 175 с.

4. Бармен С. Разработка правил информационной безопасности. - М.: Издат. дом «Вильямс», 2002 г. - 207 с.

5. Бахвалов Н.С. Численные методы. - 2003.

6. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: учеб. пособие для вузов. - М.: Горячая линия-телеком, 2006 г. - 544 с.

7. Галатенко В.А. Основы информационной безопасности. Курс лекций: рекомендовано Мин. образования. - М.: ИНТУИТ.РУ «Интернет-университет», 2003 г. - 277 с.

8. Гмурман В.Е. Теория вероятностей и мат. статистика. - 2003 г.

9. Демидович Б.П., Марон И.А. Основы вычислительной математики. - 2006 г.

10. Защита информации в системах мобильной связи: учеб. пособие для вузов / под ред. А.В. Заряева и С.В. Скрыля. - М.: Горячая линия-телеком, 2005 г. - 171 с.

11. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем: учеб. пособие. - М.: Горячая линия-телеком, 2000 г. - 451 с.

12. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. - М.: Горячая линия-телеком, 2002 г. 336 с.

13. Мамлюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: учеб. пособие. - М.: Горячая линия-телеком, 2004 г. - 280 с.

14. Мамаев М. Технологии защиты информации в Интернете: спец. справочник. - СПб.: ПИТЕР, 2002 г. - 844 с.

15. Мэйволд Э. Безопасность сетей. Шаг за шагом. - М.: СП ЭКОМ, 2005 г. - 527 с.

16. Новиков Ф.А. Дискретная математика для программистов. - 2003.

17. Норткат С. и др. Анализ типовых нарушений безопасности в сетях. - М.: Издат. дом «Вильямс», 2001 г. - 460 с.

18. Петраков А.В., Лагутин В.С. Защита абонентского телетрафика: учеб. пособие. - М.: Радио и связь, 2004 г. - 499 с.

19. Рябко Б.Я. Теория вероятностей и основы теории массового обслуживания. - 2003 г.

20. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: учеб. пособие для вузов. - М.: Горячая линия-телеком, 2005 г. - 229 с.

21. Савельев Л.Я. Элементарная теория вероятностей. - 2005 г.

22. Самарский А.А Введение в численные методы. - 2005 г.

23. Феллер В. Введение в теорию вероятностей и ее приложения, тт. 1, 2.

24. Хорев П.Б. Методы и средства защиты информации в компьютерных системах - М.: Академия, 2005 г. - 255 с.