ПРОГРАММА

ВСТУПИТЕЛЬНОГО ЭКЗАМЕНА ПО СПЕЦИАЛЬНОСТИ

2.3.6 – 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.

Основы законодательства в области защиты информации.

2. Избранные разделы математики

Методы решения систем линейных уравнений.

Методы интерполяции.

Методы численного интегрирования.

Численные методы нахождения экстремумов функций.

Элементы комбинаторики: перестановки, выборки, сочетания и размещения, биномиальные коэффициенты, их свойства.

Элементы теории графов: определение графа, способы представления, маршруты, цепи, циклы.

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

Алгебра логики, формулы, функции алгебры логики.

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

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.

Задача о линейном программировании.

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.

Основы теории чисел: Алгоритм Евклида, операции по числовому модулю

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.

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.

Задача сортировки и основные алгоритмы сортировки.

Поиск информации методом хеширования.

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

Модель криптосистемы. Принцип Кергхоффа. Типы криптосистем.

Идеальные (безусловно стойкие криптосистемы)ю Расстояниединственности. Формула Шеннона-Хеллмана.

Вычислительно стойкие шифры. Принцип постоения блоковых шифров. Схема Фейстеля. Подстановочно-перестановочные шифры. Понятие о линейном и разностном криптоанализе.

Элементы теории конечных полей.

Модификации блоковых шифров. Многократное шифрование.

Примеры построения блоковых шифров.(DES, ГОСТ.AES).

Потоковые шифры. Линейный рекуррентный регистр и его основные свойства. Нелинейные узлы усложнения. Пример построения потоковых шифров (А5/1, А/3).

Общая структура аутентификации. Безусловно стойкая система аутентификации. Вычислительно стойкие системы аутентификации. Криптографические хеш-функции и их основные свойства. Примеры построения систем аутентификации на шифрах ГОСТ.

Основные положения теории чисел.(Делимость. Алгоритм Евклида, Малая теорема Ферма. Вычисление по модулю. Основные тесты по проверке простых чисел).

Криптосистема РША (Шифрование, дешифрование, стойкость).

Криптосистема Диффи-Хеллмана и её свойства. Криптосистема Эль-Гамаля.

Метод задания криптосистем над эллиптическими кривыми.

Криптосистема Мак-Элис.

Принцип построения цифровых подписей (ЦП). ЦП на основе криптосистем РША и Эль-Гамаля.

Бесключевые хеш-функции и способы их потсроения. Стандарты ЦП.

Основные криптографические протоколы (начальные условия и целевые функции). Реализация криптопротоколов разделения секретов, доказательств с нулевым соглашением и поручительства информации.

Модель управления ключами. Распределение ключей для симметричных и нессиметричных криптосистем. Протоколы Нидхема-Шредера и Отвея-Рииса. Понятие об управлении открытыми ключами.

5. Основы стеганографии

Определение стегосистем (СГ) и систем с цифровыми водяными знаками (ЦВЗ). Покрывающие объекты. Критерии эффективности стегосистем. СГ с вложением в наименьшие значащие биты (НЗБ). СГ с использованием широкополосных сигналов. Лингвистические СГ. СГ с вложением в растровые документы. СГ в каналах с шумом. Идеальные СГ. Относительная энтропия как критерий стойкости СГ. Слепой стегоанализ.

Основные цели построения систем ЦВЗ. Примерыт построения однобитовых и многобитовых систем ЦВЗ. Аутентификация сообщений на основе использования систем ЦВЗ. ЦВЗ для аудио сигналов.

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.

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. Бахвалов Н.С. Численные методы. - 2003.
4. 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.
5. Галатенко В.А. Основы информационной безопасности. Курс лекций: рекомендовано Мин. образования. - М.: ИНТУИТ.РУ «Интернет-университет», 2003 г. - 277 с.
6. Гмурман В.Е. Теория вероятностей и мат. статистика. - 2003 г.
7. Демидович Б.П., Марон И.А. Основы вычислительной математики. - 2006 г.
8. Новиков Ф.А. Дискретная математика для программистов. - 2003.
9. Петраков А.В., Лагутин В.С. Защита абонентского телетрафика: учеб. пособие. - М.: Радио и связь, 2004 г. - 499 с.
10. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: учеб. пособие для вузов. - М.: Горячая линия-телеком, 2005 г. - 229 с.
11. Самарский А.А Введение в численные методы. - 2005 г.
12. Феллер В. Введение в теорию вероятностей и ее приложения, тт. 1, 2.
13. Коржик В.И., Яковлев В.А. Основы криптографии. Учебное пособие СПб. Изд. Интермедиа. 2016.-296 с.
14. Цифровая стеганография. Часть 1 под редакцией В.И. Коржика. СПб. 2016
15. Коржик В.И., Просихин В.П. Яковлев В.А. Основы криптографии: учебное пособие. –СПб., 2014, - 276 с.
16. Лекции по основам стеганографии. Кафедра безопасности телекоммуникационных систем. Учебные материалы Интернет.
17. Хорев П.Б. Методы и средства защиты информации в компьютерных системах - М.: Академия, 2005 г. - 255 с.

Программу составил к.т.н., доцент, зав. кафедрой ЗСС
_____ Красов А.В.

СОГЛАСОВАНО:

Проректор по научной работе А.В. Шестаков

Начальник УНРПНК А.А. Нестеров