МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Пензенский государственный университет»
(ФГБОУ ВО «ПГУ»)

«Утверждаю»
Председатель приемной комиссии,
Ректор ПГУ _____ А.Д Гуляков
31 октября 2023 г.

ПРОГРАММА
вступительного испытания для поступающих на обучение по программам подготовки научно-педагогических кадров в аспирантуре

2.3 Информационные технологии и телекоммуникации
2.3.6 Методы и системы защиты информации, информационная безопасность

Составитель
канд. тех. наук, доцент
С.Л. Зефиров

Пенза, ПГУ 2023

ОБЩИЕ ПОЛОЖЕНИЯ

Программа отражает современное состояние обеспечения информационной безопасности и включает важнейшие общенаучные разделы, знание которых необходимо специалисту в этой области. Рассмотрение проблем защиты информации и информационной безопасности базируется на задачах ускорения научно-технического прогресса и в частности – на необходимости решения данных проблем в связи с интенсивной информатизацией современного общества.

СОДЕРЖАНИЕ ПРОГРАММЫ

1. Избранные разделы математики и информатики.

1. Информация, сообщения, информационные системы и процессы как объекты информационной безопасности.
2. Основные свойства информации. Мера количества информации. Энтропия.
3. Случайные события. Полная группа событий. Зависимые и независимые случайные события. Вероятность случайного события.
4. Условная вероятность. Формула полной вероятности. Теорема Байеса.
5. Случайные величины и их характеристики: функция распределения, моменты, характеристические функции.
6. Дискретные и непрерывные случайные величины. Биноминальный закон распределения. Нормальный закон распределения.
7. Основные задачи математической статистики: точечная оценка, построение доверительного интервала, различение статистических гипотез.
8. Сетевая модель OSI/ISO. Уровни модели OSI. Примеры протоколов.

2. Теоретические основы информационной безопасности

1. Понятие угрозы информационной безопасности. Виды угроз.
2. Основные принципы обеспечения информационной безопасности (ИБ) в автоматизированных системах (АС), в телекоммуникационных системах.
3. Методы оценки угроз ИБ. Модель угроз.
4. Причины, виды и каналы утечки информации.
5. Построение систем защиты от угроз нарушения конфиденциальности информации.
6. Построение систем защиты от угроз нарушения целостности информации.
7. Построение систем защиты от угроз нарушения доступности информации.
8. Управление информационной безопасностью. Управление рисками ИБ.
9. Основные критерии защищенности АС. Классификация систем защиты АС. Руководящие документы Федеральной службы технического и экспортного контроля.

3. Основы криптографической защиты информации.

1. Криптографические методы зашиты информации. Основные понятия криптографии. Исторические шифры.

2. Теоретическая, практическая и временная стойкость системы криптографической защиты.

3. Методы получения псевдослучайных последовательностей. Современные поточные и блочные алгоритмы шифрования.

4. Системы симметричного шифрования.

5. Системы асимметричного шифрования, открытый ключ, электронная подпись.

6. Генерация и распределение ключей. Обоснование стойкости криптографической защиты.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. Теория вероятностей. Учеб. для вузов. Вентцель Е.С. - М.: Высшая школа, 1999. – 575с.

2. Теория вероятностей. Учеб. для вузов. А.В. Печинкин, О.И. Тескин, Г.М. Цветкова и др. М.: МГТУ им Н.Э Баумана, 2004 с.

3. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учеб. пособие для вузов / П.Ю. Белкин, О.О. Михальский, А.С. Першаков и др. – М.: Радио и связь, 1999. – 168 с.

4. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учеб. пособие для вузов / Проскурин В.Г., Крутов С.В., Мацкевич И.В. – М.: Радио и связь, 2000. – 168 с.

5. Алфёров А.П., Кузьмин А.С., Зубов А.Ю., Черёмушкин А.В. Основы криптографии: Учебное пособие. - М.: ГелиосАРВ, 2002. - 480с.

6. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. - Феникс, 2008. -173 с.

7. Герасименко В.А., Малюк А.А. Основы защиты информации. - М.: МОПО, МИФИ, 1997. - 537 с.

8. Теория и практика обеспечения информационной безопасности / Под ред. П. Д. Зегжды. - М.: Издательство агентства «Яхтсмен», 1996. - 192 с.

Председатель предметной
экзаменационной комиссии  С.Л. Зефиров