

ИНСТИТУТ КОМПЬЮТЕРНЫХ НАУК И ТЕХНОЛОГИЙ
ПРОГРАММА

вступительных испытаний в магистратуру по направлению
10.04.01 Информационная безопасность

Математические основы компьютерной безопасности

1. Основные алгебраические структуры и их свойства.
2. Основные понятия теории вероятностей и математической статистики (случайные величины, предельные теоремы теории вероятностей, методы оценивания параметров и проверки статистических гипотез).
3. Основные понятия математической логики (алгебра высказываний, исчисление высказываний, исчисление предикатов) и теории алгоритмов.

Методы и языки программирования

1. Принципы методы и средства проектирования архитектуры и структуры, проектирования логики, тестирования и отладки, документирования и сопровождения программного обеспечения
2. Структуры данных и абстракции данных.
3. Алгоритмы сортировки и поиска.
4. Общие принципы построения и использования языков программирования.
5. Принципы программирования на языках высокого уровня.
6. Объектно-ориентированные языки программирования.
7. Современные средства разработки программ.

Основы информационной безопасности

1. Теоретические основы компьютерной безопасности (угрозы безопасности, политики безопасности, модели безопасности).
2. Безопасность операционных систем (принципы построения, управление ресурсами, памятью, процессами, организация управления доступом и защиты ресурсов, основные механизмы безопасности).
3. Безопасность вычислительных сетей (основы организации и функционирования сетей, средства взаимодействия процессов в сетях, распределенная обработка информации в системах клиент-сервер, администрирование, безопасность ресурсов сети).
4. Криптографические методы защиты информации (простейшие шифры и их свойства, системы шифрования с открытым ключом, принципы построения криптографических алгоритмов, ключевые системы, криптографические хэш-функции, цифровая подпись).
5. Защита программ и данных (защита от вредоносного программного обеспечения, защита программ от изменения и контроль целостности, основные требования к программной и программно-аппаратной реализации средств обеспечения информационной безопасности).

Литература

1. Виноградов И. М. Основы теории чисел. Москва-Ижевск: 2003.
2. Ростовцев А.Г. Алгебра и теория чисел. Конспект лекций. СПб.: Изд-во СПбГПУ, 2011.
3. Гмурман В.Е. Теория вероятностей и математическая статистика: учеб. пособие для вузов. М.: Юрайт, 2010.
4. Шапорев С.Д. Математическая логика: курс лекций и практических занятий. СПб.: БХВ-Петербург, 2007.
5. Керниган Б. Ритчи Д. Язык программирования Си: Пер. с англ. / М.: Вильямс, 2005.
6. Кнут Д. Искусство программирования для ЭВМ. Т. 2. Получисленные алгоритмы. М.: Вильямс, 2005.
7. Вирт Н. Алгоритмы и структуры данных. СПб.: Невский Диалект, 2008.
8. Зегжда П.Д., Рудина Е.А. Основы информационной безопасности. СПб.: Изд-во Политехн. ун-та, 2008.
9. Калинин М.О. Безопасность компьютерных систем. СПб.: Изд-во Политехн.ун-та, 2010.
- 10.Корт С.С. Теоретические основы защиты информации. М.: Гелиос-АРВ, 2004.
- 11.Платонов В.В. Программно-аппаратные средства защиты информации. М.: Академия, 2013.