ФЕДЕРАЛЬНОЕ АГЕНТСТВО МОРСКОГО И РЕЧНОГО ТРАНСПОРТА

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

МОРСКОЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

имени адмирала Г.И. Невельского

ФИЗИКО-ТЕХНИЧЕСКИЙ ФАКУЛЬТЕТ

ОДОБРЕНО
Ученым советом
Морского института
информационных технологий
Председатель ученого совета института (факультета)

(подпись) / С.В. Глушков / (ФИО)

29 января 2016г.
дата

УТВЕРЖДАЮ
Проректор по научной работе

(подпись) / О.А. Букин / (ФИО)

29 января 2016 г.
дата

ПРОГРАММА ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ
по специальной дисциплине

Методы и системы защиты информации, информационная безопасность
(наименование дисциплины)

Направление подготовки *10.06.01 «Информационная безопасность»*
(шифр и наименование)

Уровень образования подготовка кадров высшей квалификации

Профиль *05.13.19 «Методы и средства защиты информации, информационная безопасность»*
(шифр и наименование)

Сформирована на основе федеральных государственных образовательных стандартов высшего образования по программам специалитета и магистратуры

Программа вступительных испытаний обсуждена на заседании кафедры

Безопасности информации и телекоммуникационных систем

протокол от 19 октября 2015 № 2

Заведующий кафедрой (подпись) / *Е.А. Верещагина* / (ФИО)

Разработал *к.п.н., доцент И.А. Щербинина*
(степень, звание, И.О. Фамилия)

1. МАТЕМАТИЧЕСКИЙ АНАЛИЗ

1. Непрерывность действительных функций одного и многих действительных переменных. Свойства непрерывных функций.
2. Дифференцируемость функций одного и многих действительных переменных в точке и на множестве. Достаточные условия дифференцируемости. Производные и дифференциалы высших порядков.
3. Теоремы о среднем для действительных функций одного действительного переменного (Ролля, Лагранжа, Коши) и их применение.
4. Формула Тейлора для действительных функций одного и многих действительных переменных и ее применение. Экстремум действительной функции одного и многих действительных переменных, достаточные условия его существования.
5. Числовой ряд. Сходящиеся ряды и их простейшие свойства. Признаки сходимости рядов с положительными членами (признаки сравнения, Даламбера, Коши). Абсолютно и не абсолютно сходящиеся ряды. Признак Лейбница. Переместительное свойство абсолютно сходящихся рядов.
6. Функциональные ряды. Равномерно сходящиеся ряды. Критерий Коши равномерной сходимости ряда. Непрерывность суммы равномерно сходящегося ряда непрерывных функций.
7.

2. ТЕОРИЯ ВЕРОЯТНОСТЕЙ И МАТЕМАТИЧЕСКАЯ СТАТИСТИКА

7. Вероятностное пространство. Аксиомы теории вероятностей. Классическое определение вероятности.
8. Случайные величины, функции распределения, их свойства. Абсолютно непрерывные и дискретные распределения. Типовые распределения: биномиальное, пуассоновское, нормальное, x^2~Р^{асп}Р^{е}Д^{еление}- Схема Бернулли и полиномиальная схема: основные формулы.
9. Условные вероятности. Независимость событий. Формула полной вероятности. Формулы Байеса. Независимые случайные величины.
10. Математическое ожидание случайной величины и его свойства. Примеры.
    Дисперсия случайной величины и ее свойства. Вычисление математических ожиданий и дисперсий типовых распределений.
11. Виды сходимости последовательностей случайных величин. Закон больших чисел. Теорема Чебышева.
12. Центральная предельная теорема для независимых одинаково распределенных случайных величин.
13. Основные понятия математической статистики: случайная выборка из распределения, выборочное пространство, вариационный ряд, эмпирическая функция распределения, выборочное среднее, выборочные дисперсии, выборочные моменты. Точечные оценки неизвестных значений параметров распределений: несмещенные оценки, состоятельные оценки. Примеры.
14. Задача проверки статистических гипотез. Основная и альтернативная, про-

стая и сложная гипотезы. Статистические критерии. Ошибки 1-го и 2-го родов при проверке гипотез. Функция мощности критерия. Наиболее мощный и равномерно наиболее мощный критерии. Лемма Неймана-Пирсона. Проверка простых гипотез о параметрах биномиального, полиномиального и нормального распределений.

15. Критерии согласия. Критерий согласия Пирсона (критерий j^2). Теорема Пирсона о предельном распределении % -статистики (без доказательства).

3. АЛГЕБРА

16. Матрицы над кольцом и операции над ними. Кольцо квадратных матриц. Определители матриц и их свойства. Разложение определителя по строке (столбцу). Определитель произведения матриц. Критерий обратимости матрицы надкоммутативным кольцом с единицей.
17. Ранг матрицы над полем, способы его вычисления. Ранг произведения матриц. Обратная матрица и способы ее вычисления.
18. Векторные пространства над полем. Линейно зависимые и независимые системы векторов. Подпространства векторного пространства, операции над ними. Свойства конечномерных векторных пространств. Координаты векторов в базисе и их изменение при переходе к другому базису. Размерности суммы и пересечения подпространств.
19. Системы линейных уравнений над полем. Алгоритм Гаусса. Критерий Кроне- кера-Капелли. Фундаментальная система решений системы линейных однородных уравнений. Общее решение системы линейных уравнений.
20. Кольцо многочленов над кольцом с единицей. Делимость многочленов с остатком. Теорема Безу.
21. Наибольший общий делитель (НОД) и наименьшее общее кратное (НОК) многочленов над полем. Свойства НОД и алгоритм его нахождения. Взаимно простые многочлены и их свойства. Неприводимые многочлены и их свойства. Каноническое разложение многочлена и его однозначность.
22. Линейное преобразование конечномерного векторного пространства, его матрица в данном базисе, примеры. Критерии обратимости преобразования.
23. Характеристический многочлен линейного преобразования. Собственные значения и собственные векторы преобразования, инвариантные подпространства. Критерий приводимости и разложимости матрицы преобразования.
24. Конечные поля, характеристика поля, число элементов, теорема о примитивном
элементе. Существование поля с заданным примарным числом элементов. Описание подполей.
25. Неприводимые многочлены над конечными полями. Существование неприводимых многочленов данной степени над конечным полем. Построение конечного поля с заданным числом элементов.

4. ТЕОРИЯ ИНФОРМАЦИИ И КОДИРОВАНИЯ

26. Энтропия и ее свойства. Количество информации.
27. Источник сообщения, его энтропия и избыточность.
28. Модель канала связи. Пропускная способность канала связи.
29. Оптимальное кодирование. Корректирующие свойства кодов.
30. Линейный код и способы его задания. Процесс декодирования линейного кода. БЧХ-коды. Код Хемминга.

Раздел 5. ЗАЩИТА ИНФОРМАЦИИ

31. Основные понятия защиты информации (субъекты, объекты, доступ, граф доступов, информационные потоки). Постановка задачи построения защищенной автоматизированной системы (АС). Модели ценности информации. Аддитивная модель. Порядковая шкала. Модель решетки ценности. *MLS* решетка.
32. Угрозы безопасности информации. Угрозы конфиденциальности, целостности, доступности, раскрытия параметров АС. Понятие политики безопасности. Дискреционная политика безопасности. Мандатная политика безопасности. Мандатная политика целостности.
33. Модель системы безопасности *HRU.* Основные положения модели. Теорема об алгоритмической неразрешимости проблемы безопасности в произвольной системе.
34. Модель распространения прав доступа *Take-Grant.* Теоремы о передаче прав в графе доступов, состоящем из субъектов, и произвольном графе доступор. Расширенная модель *Take-Grant* и ее применение для анализа информационных потоков в АС.
35. Модель Белла-Лападулы как основа построения систем мандатного разграничения доступа. Основные положения модели. Базовая теорема безопасности *(BST).*
36. Основные положения критериев *TCSEC* ("Оранжевая книга"). Фундаментальные требования компьютерной безопасности. Требования классов защиты.
37. Основные положения Руководящих документов ГТК в области защиты информации. Определение и классификация НС Д. Определение и классификация нарушителя. Классы защищенности АС от НСД к информации.
38. Основные положения *CCITSE* ("Единые критерии"). Структура профиля и проекта защиты. Структура и ранжирование функциональных требований. Структура требований адекватности и уровни адекватности.
39. Криптосистемы с открытым ключом. Понятие сертификата. Криптосистема *RSA.* Выбор параметров.
40. Криптографические хэш-функции. Стандарты ГОСТ Р 34.11 и *SHA.*
41. Цифровая подпись. Схемы цифровой подписи. Стандарты ГОСТ Р 34.10 и *DSS.*
42. Криптографические протоколы.
43. Структуры данных и основные алгоритмы поиска и сортировки.

44. Программно-аппаратные средства обеспечения информационной безопасности в компьютерных сетях.
45. Классификация и возможности видов технической разведки

Список рекомендуемой литературы

1. Основная литература

1. Мартемьянов Ю.Ф., Яковлев Ал.В., Яковлев Ан.В. Операционные системы. Концепции построения и обеспечения безопасности Учебное пособие [Электронный ресурс] : — Электрон. дан. — Горячая линия – Телеком.2011 Москва Количество — 332 с. ISBN: гриф УМО — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5176
2. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками Учебное пособие для вузов [Электронный ресурс] : — Электрон. дан. — Горячая линия – Телеком 2013 Москва — 338с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5150
3. Питер Нортон, Джон Мюллер Полное руководство по Microsoft Windows XP [Электронный ресурс] : — Электрон. дан. — ДМК Пресс, 2007 Москва практическое руководство — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=1195

4. Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие. [Электронный ресурс] : — Электрон. дан. — М.: Изд.центр «Академия», 2012. — 144 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=63235

2. Дополнительная литература

1. Шелухин О.И., Сакалема Д.Ж., Филинова А.С.Обнаружение вторжений в компьютерные сети (сетевые аномалии) Учебное пособие для вузов [Электронный ресурс] : — Электрон. дан. — Горячая линия - Телекомред. Шелухин О.И. 2013 Москва — 220 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=11849
2. Ховард М., Лебланк Д., Виега Д. 19 смертных грехов, угрожающих безопасности программ. Как не допустить типичных ошибок [Электронный ресурс] : — Электрон. дан. — ДМК Пресс 2008 Москва — 288 с. практическое пособие — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=1118
3. Курячий Г.В., Маслинский К.А. Операционная система Linux. Курс лекций Учебное пособие [Электронный ресурс] : — Электрон. дан. — ДМК Пресс 2010 Москва — 348 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=1202