Министерство образования Республики Беларусь

Учреждение образования
"БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ"

УТВЕРЖДАЮ
Проректор по учебной работе
_____ А.А. Хмыль
«_15__» «___05_____» 2014г.

ПРОГРАММА

вступительного экзамена в магистратуру по специальности
1-98 80 01 "Методы и системы защиты информации, информационная безопасность"

Минск, 2014

Программа составлена на основании типовых учебных программ дисциплины:

Основы защиты информации.
Регистрационный № ТД-1.013 от 27.02.2006г.

Защита объектов связи от несанкционированного доступа.
Регистрационный № ТД-Р.210/тип.от 03 марта 2010 г.

Защита информации в банковских технологиях.
Регистрационный № ТД-Р.333/тип.от 14.06.2011 г.
Специальности (ей) 98 01 02 «Защита информации в телекоммуникациях»

Составители:

Борботько Т.В. – к.т.н., доцент , кафедра ЗИ

Лыньков Л.М. – д.т.н., профессор, зав. каф. ЗИ

РЕКОМЕНДОВНА К УТВЕРЖДЕНИЮ

Кафедрой защиты информации учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (протокол № 16 от 15 .05.2014).

Заведующий кафедрой ЗИ, Л.М.Лыньков
д.т.н., профессор

Раздел 1. **Математические основы информационной безопасности**

Тема 1.1. Функциональный анализ

Метрические пространства. Сепарабельные пространства. Нормированные пространства. Гильбертово пространство. Аддитивные операторы, линейные операторы, ограниченность линейных операторов, обратные операторы, матричные линейные операторы. Линейные функционалы. Приближенное решение функциональных уравнений. Замена точного уравнения «приближенным». Замена произвольного интегрального уравнения на уравнение с вырожденным ядром.

Тема 1.2. Алгебра и теория чисел

Теория делимости в кольце целых чисел. Сравнения. Малая теорема Ферма и теорема Эйлера. Первообразные корни, индексы. Символ Лежандра. Квадратичный закон взаимности Гаусса. Символ Якоби. Решение квадратичных сравнений по простому модулю. Асимптотический закон распределения простых чисел. Конечные поля и их свойства. Детерминированные и вероятностные методы тестирования на простоту. Тест Лемера-Поклингтона. Тест Миллера-Рабина. Экспоненциальные методы факторизации целых чисел. Конечные расширения. Кольца целых алгебраических чисел. Модули, идеалы, порядки в кольцах целых алгебраических чисел. Факториальные кольца. Группы классов. Эллиптические функции. Функция Вейерштрасса. Уравнение эллиптической кривой в форме Вейерштрасса. Группа точек эллиптической кривой. Инварианты эллиптической кривой.

Тема 1.3. Теория вероятностей, теория случайных процессов и математическая статистика

Аксиоматика А.Н. Колмогорова. Вероятностное пространство. Условные вероятности. Полная вероятность событий. Непрерывные случайные величины и их распределения. Функции распределения вероятностей. Законы распределения вероятностей. Интеграл Лебега по вероятностной мере. Числовые характеристики случайных величин. Моменты распределения случайных величин. Случайные вектора. Распределение компонент случайного вектора. Многомерное нормальное распределение. Полиномиальное распределение. Характеристические функции случайных величин. Случайные последовательности. Законы больших чисел. Усиленный закон больших чисел. Предельные теоремы теории вероятностей. Стационарные случайные процессы. Марковские процессы. Винеровский процесс. Дискретные случайные процессы. Процесс независимых испытаний с двумя исходами. Законы распределения дискретных случайных процессов. Марковские цепи. Задачи математической статистики. Несмещенные оценки математического ожидания и дисперсии случайной величины. Метод Монте-Карло. Несмещенные оценки математического ожидания и ковариационной матрицы случайного вектора. Нахождение оценок по методу максимального правдоподобия. Оценки максимального правдоподобия параметров конечной цепи Маркова. Оценка

параметров по методу доверительных интервалов. Статистическая проверка гипотез. Критерий согласия. Регрессионный анализ и планирование эксперимента. Определение коэффициентов регрессии по данным пассивного эксперимента. Понятие о планировании эксперимента. Робастность статистических выводов.

Тема 1.4. Дискретная математика

Операции на множествах и их свойства. Полугруппы, группы, решетки. Функции алгебры логики. Булева алгебра. Полнота и замкнутость. Язык логики предикатов. Графы, основные понятия и операции, маршруты, цепи и циклы. Некоторые классы графов и их частей. ориентированные графы. Графы с помеченными вершинами и ребрами.

Теория алгоритмов. Машина Тьюринга, обобщенная машина Тьюринга, рекурсивные функции, вычислимость и разрешимость.

Формальные системы. Формальные теории. Исчисления высказываний. Исчисление предикатов и теории первого порядка. Метатеория логических исчислений. Абстрактные формальные системы. Языки и грамматики. Формальные грамматики и их свойства. Операции над языками. Семантика формальных языков.

Автоматы. Основные понятия. Распознавание множеств автоматами. Сети из автоматов, их анализ и синтез. Программная реализация логических функций и автоматов.

Комбинаторные задачи. Классы трудоемкости комбинаторных задач. Метод ветвей и границ. Линейное программирование.

Раздел 2. Распознавание образов

Вероятностные модели классифицируемых данных. Байесовское решающее правило. Оптимальная классификация многомерных гауссовских наблюдений. Подстановочные решающие правила. Непараметрические классификаторы. Метод “*k* ближайших соседей”. “Обучение ” и “самообучение” при построении алгоритмов распознавания. Генетические алгоритмы и нейронные сети. Методы построения информативных признаков. Алгоритмы кластер-анализа.

Раздел 3. Теория кодирования

Основные понятия кодирования. Общая модель цифровой системы связи. Модели каналов связи.

Декодирование по методу максимального правдоподобия. Типы кодов. Метрики. Блоковые коды . Древовидные коды. Описание кодов при помощи матриц. Сверточные коды. Систематические коды. Стандартное расположение таблиц декодирования. Теорема о вероятности правильного декодирования. Поэтапное декодирование. Эквивалентность линейных кодов.

Распределение весов. Максимально разнесенные коды. Исправление ошибок при помощи линейных кодов. Границы минимального расстояния. Границы вероятности ошибочного декодирования. Свойства и значения границ

для различных типов кодов.

Оптимизация кодов. Основной критерий оптимизации кодов.

Раздел 4. Теория информации

Источники дискретных сообщений и их вероятностные модели. Функционал энтропии и его свойства. Условная энтропия. Энтропийные характеристики Марковских последовательностей. Источники непрерывных сообщений и их энтропийные свойства. Оптимизация энтропии на классе вероятностных распределений. Асимптотические свойства стационарного источника дискретных сообщений. Энтропийная устойчивость последовательностей. Количество информации и его свойства. Шенноновские модели криптосистем. Теоретико-информационные оценки стойкости криптосистем. Оптимальное кодирование при наличии шума. Основная теорема для дискретного канала с шумом. Избыточность. Пропускная способность дискретного канала.

Раздел 5. Методы криптологии

Алгебраические и теоретико-числовые методы в криптологии. Идеальные шифры. Шифр Вернама. Симметричные криптосистемы. Криптосистема DES. Разностный криптоанализ DES. Линейный криптоанализ DES. Криптосистемы IDEA, ГОСТ. Односторонняя функция с ключом. Асимметричные криптосистемы. Криптосистема RSA. Генерация простых чисел в криптосистемах типа RSA. Методы факторизации целых чисел. Цифровая подпись. Схемы цифровой подписи Рабина, Эль Гамаля, DSS. Методы дискретного логарифмирования в конечных полях. Функции хэширования. Методы построения коллизий для функций хэширования. Криптографические протоколы. Протоколы аутентификации. Протоколы генерации ключей. Протоколы распределения ключей без участия третьей доверенной стороны. Схема Диффи-Хеллмана. Протоколы распределения ключей с участием третьей доверенной стороны. Протокол Kerberos. Генераторы случайных последовательностей. Статистическое тестирование случайных последовательностей. Квантовая криптография.

Раздел 6. Основы информационной безопасности

Информационная безопасность. Критерии оценки безопасности информационных технологий. Информационные системы и объекты информатизации – объекты информационной безопасности, особенности структуры их построения и анализа. Классификация информационных систем по степени безопасности. Каналы утечки и компрометации информации. Угрозы информационной безопасности, их классификация, характер проявления и возможные последствия от проявления угроз. Обобщенная модель нарушителя. Методы оценки риска. Методы обнаружения, локализации и ликвидации угроз информационной безопасности. Общие требования по обеспечению информационной безопасности. Профиль защиты и задание по обеспечению безопасности, их структура и взаимосвязи между ними. Политика

и задачи безопасности, их взаимосвязь. Функциональные и гарантийные требования безопасности. Анализ безопасности программ. Методы анализа безопасности программного обеспечения. Логико-аналитические методы анализа безопасности программного обеспечения. Модели разграничения доступа. Методы контроля доступа. Модели контроля целостности. Модель Биба. Модель Кларка-Вилсона. Политика безопасности. Дискреционная политика безопасности. Многоуровневая политика безопасности. Классификация систем защиты информации. «Оранжевая книга».

Раздел 7. Технические каналы утечки информации

Причины образования технических каналов утечки информации. Источники образования технических каналов утечки информации. Прямой перехват сигналов. Индуктивные и емкостные акустоэлектрические преобразователи. Емкостные преобразователи. Микрофонный эффект. Пьезоэлектрический эффект. Излучатели электромагнитных колебаний. Оптические излучатели. Классификация технических каналов утечки информации. Паразитные связи и наводки. Паразитные емкостные связи. Паразитные индуктивные связи. Паразитные электромагнитные связи. Паразитные электромеханические связи. Обратная связь в усилителях. Утечка информации по линиям питания. Утечка информации по цепям заземления. Взаимные влияния в линиях связи. Несанкционированный доступ в электромагнитных каналах. Способы незаконного подключения к линиям связи. Высокочастотное навязывание. Утечка информации по прямому акустическому каналу. Защита информации от утечки по прямому акустическому каналу. Утечка информации в оптических каналах связи. Методы обнаружения устройств контроля, использующих электромагнитный канал. Нелинейная локация. Сканирующие радиоприемники. Генераторы шума. Излучающие системы. Нейтрализация устройств магнитной записи. Выжигатели телефонных закладных устройств. Подавление информационных сигналов электромагнитных излучений и наводок. Сетевые фильтры для питания. Защита телефонных аппаратов. Средства поиска и обнаружения радиозакладных устройств. Защита линий связи и связной аппаратуры. Экранирование узлов радиоэлектронной аппаратуры и их соединений. Трансформаторы, катушки и фильтры. Защита электронных усилительных устройств. Антенно-фидерные устройства. Экранирование электромагнитных полей. Экранированные помещения и кабины. Соединение отдельных блоков. Методы создания электромагнитных экранов. Основные принципы конструирования экранов. Металлические экраны. Сетчатые экраны. Конструктивно-технологические особенности создания радиопоглощающих материалов. Гибкие конструкции электромагнитных экранов и радиопоглощающих покрытий и их применение. Электромагнитное заземление. Согласованные нагрузки. Акустическая, оптическая и радиоэлектронная маскировка.

Раздел 8. Обеспечение безопасности информации в

телекоммуникационных системах (ТКС)

Модели разграничения доступа к информации. Методы разграничения доступа. Обеспечение целостности данных в ТКС. Особенности обеспечения безопасности информации в ТКС. Классификация угроз безопасности информации в ТКС. Угрозы, возникающие вследствие преднамеренных действий персонала. Угрозы, возникающие вследствие случайных несанкционированных действий персонала. Угрозы, возникающие вследствие отказов элементов технических средств. Модели защиты каналов. Алгоритм работы средств защиты. Функции средств защиты каналов доступа. Параметры средства защиты каналов доступа. Модель разграничения доступа к защищаемым сведениям. Схема распределения сведений. Алгоритмы анализа правил разграничения доступа. Алгоритм построения матрицы разграничения доступа к защищаемым данным. Модель управления доступом к массивам данных. Представление алгоритмов управления доступом с учётом параметров ТКС. Методы опознания и установления подлинности. Опознание на основе принципов "что знает субъект", "что имеет субъект", "что присуще субъекту". Методы опознания с использованием криптографии и их реализация. Опознание локальных объектов и объектов в распределенной сети с помощью криптографических методов. Методы управления доступом и способы их реализации. Анализ возможности обеспечения целостности данных. Способы обеспечения целостности данных. Методология проверки целостности множества двоичных данных. Полиномиальная свертка. Использование механизма целостности данных для имитозащиты сообщений в ТКС. Имитозащита сообщений в ТКС. Функциональная и кодовая независимость контрольных комбинаций при имитозащите широковещательных сообщений.

Раздел 9. Защита объектов от несанкционированного доступа.

Структура и основные элементы. Технические средства. Системы и средства охраны, видеонаблюдения, контроля доступа. Этапы управления и элементы системы. Техническая дезинформация. Скрытие сигналов радиоэлектронных средств. Видовая разведка. Контроль эффективности противодействия. Технический контроль зашиты информации.

Литература

К разделу 1

1. Вулих Б.З. Введение в функциональный анализ. – М.: Изд-во физико-математической литературы, 1968.
2. Комогоров А.Н., Фомин С.В. Элементы теории функций и функционального анализа. – М.: Наука, 1978.
3. Марчук Г.Н. Методы вычислительной математики. – М.: Наука, 1980.
4. Яблонский С.В. Введение в дискретную математику. – М.: Наука, 1986.
5. Ивченко Г.И., Медведев Ю.И. Математическая статистика. – М.: Высшая школа, 1992.
6. Харин Ю.С., Берник В.И., Матвеев Г.В. Математические основы

криптологии: Учебное пособие. – Мн.: БГУ,1999.

7. Виноградов И.М. Основы теории чисел.

8. Нестеренко Ю.В., Галочкин А.И., Шидловский А.Б. Введение в теорию чисел.

9. Лидл Р., Нидеррайтер Г. Конечные поля. – М.: Мир, 1998.

10. Koblitz N. Course in Number Theory and Cryptography, Springer-Verlag.: New York, 1987.

11. Cohen H. A Course in Computation Algebraic Number Theory. GTM 138. Springer-Verlag.: New York, 1993.

12. Боревич З.И., Шафаревич И.Р. Теория чисел. – М.: Наука, 1972.

13. Ленг С. Эллиптические функции. – М.: Наука, 1984.

14. Теория прикладного кодирования. // Под редакцией Конопелько В.К.: Учебное пособие. - Мн.: БГУИР, 2004.

15. Технические методы и средства защиты информации / Ю.Н. Максимов, В.Г. Сонников, В.Г. Петров и др. СПб.: ООО “Издательство Полигон”, 2000.

К разделу 2

1. Дуда Р., Харт П. Распознавание образов и анализ сцен. – М.: Мир, 1976.

2. Фу К. Структурные методы в распознавании образов. – М.: Мир, 1987.

3. Фукунага К. Введение в статистическую теорию распознавания образов. – М.: Наука, 1979.

4. Устройства для защиты объектов и информации / В.И. Андрианов, А.В. Соколов. СПб.: ООО “Издательство Полигон”, 2000.

К разделу 3

1. Питерсон В. Теория кодов, исправляющих ошибки. – М.: Мир, 1984.

2. Залманзон Л.А. Преобразование Фурье, Уолша, Хаара и их применения в управлении, связи и других областях. – М.: Наука, 1989.

3. Туманян Г.Б. Кодирование и декодирование сообщений. – М.: Наука, 1981.

4. Кларк Дж., Кейн Дж. Кодирование с использованием ошибок в системах цифровой связи. – М.: Радио и связь, 1987.

Берлекэмп Э. Алгебраическая теория кодирования. – М.: Мир, 1971.

К разделу 4

1. Шеннон К. Работы по теории информации и кибернетики. – М.: Наука, 1963.

2. Галлагер Р. Теория информации и надежная связь. – М.: 1974

3. Стратанович Р.Л. Теория информации. – М.: Наука, 1975.

4. Харин Ю.С., Берник В.И., Матвеев Г.В. Математические основы криптологии: Учебное пособие. – Мн.: БГУ, 1999.

5. Электронные средства коммерческой разведки и защита информации / Е.А. Рудометов, В.Е. Рудометов. СПб.: ООО “Издательство Полигон”, 2000.

К разделу 5

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С. Основы криптографии. – М.: Гелиос, 2001.

2. Варфоломеев А.А., Пеленицын М.М. Методы криптографии и их применение в банковских технологиях. – М.: МИФИ, 1995.

3. Варфоломеев А.А., Доминина О.С., Пеленицын М.Б. Управление ключами в системах криптографической защиты банковской информации. – М.: МИФИ, 1996.

4. Харин Ю.С., Берник В.И., Матвеев Г.В. Математические основы криптологии: Учебное пособие. – Мн.: БГУ, 1999.

5. Методы информационной защиты объектов и компьютерных сетей / А.В. Соколов, О.М. Степанюк. СПб.: ООО “Издательство Полигон”, 2000.

К разделу 6

1. Коллинз Г., Блей Дж. Структурные методы разработки систем. – М.: Финансы и статистика, 1986.

2. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информациии

3. Герасименко В.А., Малюк А.А. Основы защиты информации. – М.: 1997.

4. Макаров В.Ф. Теоретические основы передачи и защиты информации в системах теледоступа к вычислительным ресурсам. – М.: Академия МВД РФ, 1992.

5. Зегжда П.Д. и др. Теория и практика обеспечения информационной безопасности. – М.: Яхтсмен, 1996.

6. Компьютерная преступность и информационная безопасность. – Минск, Арил, 2000.

7. Вартанесян В.А. Радиоэлектронная разведка. – М.: Воениздат, 1991.

8. Закон РФ “Об информации, информатизации и защите информации”. М., 1995.

К разделу 7

1. В.А. Богуш, Т.В. Борботько, А.В. Гусинский и др. Электромагнитные излучения. Методы и средства защиты / Под общ. ред. Л.М. Лынькова. - Мн.: Бестпринт, 2003.

2. Боголепов Н.Г. Промышленная звукоизоляция. – М.: Судостроение, 1987.

К разделу 8

1. Бобов М.Н., Конопелько В.К. Обеспечение безопасности информации в телекоммуникационных системах / Под общ. ред. В.К. Конопелько. - Мн.: БГУИР, 2002.

2. Хаусли Т. Системы передачи и телеобработки данных. – М.: радио и связь, 1994.

3. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных сетях. – М.: Радио и связь, 2001.

4. В.А. Герасименко. Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1994., книга 1.

5. Организационно-технические методы контроля защиты информации в объектах ЭВТ: Учебное пособие. – СПб.: ВИКА, 1994.

6. Спесивцев А.В., Вегнер А., Кутяков А.Ю. Защита информации в персональных ЭВМ. – М.: Радио и связь, МП “Веста”, 1992.

К разделу 9

1. Кутин Г.И., Кузнецов А.С. Охраняемые сведения и демаскирующие признаки при противодействии техническим разведкам. - Л.: МО, 1989.

2. Макаров Г.И. Оборудование для автоматических систем контроля доступа. – М.: Формула безопасности, 1997.

3. Зубак А.Д. Извещатели оптронно-пожарной сигнализации: Учебное пособие. – Воронеж: Воронежская высшая школа МВД РФ, 1995.

4. Как сберечь свои секреты / В.И. Андрианов, А.В. Соколов. СПб.: ООО “Издательство Полигон”, 2000.

5. Электронные устройства двойного применения / Е.А. Рудометов, В.Е. Рудометов. СПб.: ООО “Издательство Полигон”, 2000.

6. Вартанесян В.И. Радиоэлектронная разведка. Военное издательство, 1991.