Министерство образования Республики Беларусь

Учреждение образования
"БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ"

УТВЕРЖДАЮ
Первый проректор
_____ С.К.Дик
«___» _____ 2018 г.

ПРОГРАММА

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

Минск, 2018

Программа составлена на основании типовых учебных программ дисциплин:

«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»

Форма экзамена: устный

Составители:

Борботько Т.В. – д.т.н., профессор, зав.кафедрой ЗИ

Лыньков Л.М. – д.т.н., профессор кафедры ЗИ

РЕКОМЕНДОВНА К УТВЕРЖДЕНИЮ

Кафедрой защиты информации учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» (протокол № 16 от 21 марта 2018 г.).

Заведующий кафедрой ЗИ,
д.т.н., профессор  Т.В.Борботько

Раздел 1. Математические основы информационной безопасности

Метрические пространства. Детерминированные и вероятностные методы тестирования на простоту. Непрерывные случайные величины и их распределения. Функции распределения вероятностей. Законы распределения вероятностей. Числовые характеристики случайных величин. Моменты распределения случайных величин. Случайные вектора. Многомерное нормальное распределение. Полиномиальное распределение. Характеристические функции случайных величин. Случайные последовательности. 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. Генетические алгоритмы и нейронные сети. Методы построения информативных признаков. Алгоритмы кластер-анализа. 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 2. Программно-техническая защита информации

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 распределения ключей Диффи-Хеллмана. Протоколы распределения ключей с участием третьей доверенной стороны. Протокол Kerberos. Генераторы случайных последовательностей. Статистическое тестирование случайных последовательностей. Квантовая криптография.

Классификация информационных систем по степени безопасности. Обобщенная модель нарушителя. Методы оценки риска. Профиль защиты и задание по обеспечению безопасности, их структура и взаимосвязи между ними. Политика и задачи безопасности, их взаимосвязь. Функциональные и гарантийные требования безопасности. Методы анализа безопасности программного обеспечения. Модели разграничения доступа. Методы контроля доступа. Модели контроля целостности. Модель Биба. Модель Кларка-Вилсона. Дискреционная политика безопасности. Многоуровневая политика безопасности.

Раздел 3. Инженерно-техническая защита информации

Информация и формы представления. Охраняемые сведения и демаскирующие признаки. Классификация угроз безопасности. Технология добывания информации. Способы доступа к источникам информации. Система защиты информации. Методы защиты информации. Категорирование объектов. Инженерные заграждения. Технические средства охраны. Системы контроля и управления доступом. Управляемые преграждающие устройства систем контроля и управления доступом. Системы пожарной сигнализации. Пожарные извещатели. Приемно-контрольные приборы систем пожарной сигнализации. Исполнительные устройства систем пожарной сигнализации. Структура системы видеонаблюдения. Классификация технических каналов утечки информации. Акустические каналы утечки информации. Акустоэлектрические преобразователи. Способы подключения к линиям связи для перехвата речевой информации. Высокочастотное навязывание. Звукоизоляция. Акустическая маскировка. Электромагнитные каналы утечки информации. Паразитные связи и наводки. Утечка информации по линиям электропитания. Утечка информации по цепям заземления. Экранирование электромагнитных полей. Конструкции электромагнитных экранов. Электромагнитное зашумление. Фильтрация сигналов наводок в проводных линиях. Специальные проверки и порядок их проведения. Специальные обследования выделенных помещений. Особенности формирования визуально-оптического канала утечки информации. Методы и средства снижения заметности объектов.

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. Виноградов И.М. Основы теории чисел.

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

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

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

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

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

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

К разделу 2

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. Шаньгин В. Информационная безопасность компьютерных систем и сетей. – М.: Форум, 2011.

6. Мартемьянов Ю.Ф. Яковлев Ал.В., Яковлев А.В. Операционные системы. Концепции построения и обеспечения безопасности.– М.: Горячая линия - Телеком, 2011.

К разделу 3

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

2. Торокин А.А. Инженерно-техническая защита информации. – М.: Гелиос АРВ, 2005.

3. Магауенов Р.Г. Системы охранной сигнализации: основы теории и принципы построения: Учеб. пособие. – М.: Горячая линия - Телеком, 2004.

4. Синилов В.Г. Системы охранной, пожарной и охранно-пожарной

сигнализации. – М.: Академия, 2010.

5. Дамьяновски В. CCTV. Библия видеонаблюдения. Цифровые и сетевые технологии. – М.: ООО "Ай-Эс-Эс Пресс", 2006.

6. Гедзберг Ю.М. Охранное телевидение. М.: Горячая линия - Телеком, 2006.

7. Меньшаков Ю.К. Защита объектов и информации от технических средств разведки. М. : Российский государственный гуманитарный университет, 2002.

8. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. М. : Горячая линия - Телеком, 2014.

9. Зайцев А.П. Технические средства и методы защиты информации. М. : Горячая линия - Телеком, 2012.