МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное бюджетное государственное образовательное учреждение высшего профессионального образования

«Тамбовский государственный технический университет»

УТВЕРЖДАЮ
И.о. ректора университета
_____ С.И. Дворецкий
«_17_» _марта_ 2014 г.
Вводится в действие с
«_31_» _марта_ 2014 г.

ПРОГРАММА

вступительного экзамена в аспирантуру по специальной дисциплине

Направление 10.06.01 Информационная безопасность

(Специальность 05.13.19 Методы и системы защиты информации, информационная безопасность)

Форма обучения:

Очная, заочная

Составитель:

кафедра «Информационные системы и защита информации»

профессор, д.т.н., Громов Юрий Юрьевич

Тамбов 2014

СОГЛАСОВАНО

Начальник управления подготовки и аттестации кадров высшей квалификации ФГБОУ ВПО «ТГТУ»

_____ Е.И. Муратова

« 13 » *марта* 2014 г.

Программа вступительного экзамена в аспирантуру по *10.06.01 Информационная безопасность* разработана в соответствии с требованиями к уровню освоения выпускниками основных образовательных программ высшего профессионального образования (специалитет, магистратура) профессионального цикла дисциплин по направлению *Информационная безопасность*.

Программа рассмотрена и утверждена на заседании Научно-технического совета университета протокол № *1* от «*13*» *марта 2013* г.

Зам председателя Научно-технического совета университета _____ М.Н. Краснянский

ПЕРЕЧЕНЬ ВОПРОСОВ

1. Основные понятия и принципы теории информационной безопасности.
2. Угрозы информационной безопасности, их анализ.
3. Виды информации, методы и средства обеспечения информационной безопасности.
4. Методы нарушения конфиденциальности, целостности и доступности информации.
5. Основы комплексного обеспечения информационной безопасности.
6. Модели, стратегии и системы обеспечения информационной безопасности.
7. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.
8. Лицензирование и сертификация в области защиты информации.
9. Правовые основы защиты информации с использованием технических средств.
10. Защиты интеллектуальной собственности.
11. Основы законодательства в области защиты информации.
12. Методы решения систем линейных уравнений.
13. Методы интерполяции.
14. Методы численного интегрирования.
15. Методы численного решения дифференциальных уравнений.
16. Численные методы нахождения экстремумов функций.
17. Элементы комбинаторики: перестановки, выборки, сочетания и размещения без повторений.
18. Сочетания и размещения с повторениями, биномиальные коэффициенты, их свойства. Элементы теории графов: определение графа, способы представления.
19. Изоморфизм графов, элементы графов, валентность, маршруты, цепи, циклы.
20. Связность графов, подграфы, виды графов (тривиальные и полные; двудольные; планарные; направленные орграфы и сети) и операции над ними.
21. Алгебра логики, формулы алгебры логики, высказывания и операции, построение формул.
22. Булевы функции и формулы, функции алгебры логики, способы представления БФ, нормальные формы.
23. Карты Карно, минимизация БФ с помощью карт Карно.
24. Теоремы сложения и умножения вероятностей.
25. Формула полной вероятности и Байеса.
26. Схема Бернулли, приближенные вычисления в схеме Бернулли.
27. Случайные величины, математическое ожидание и дисперсия.
28. Основные законы распределения случайной величины.
29. Многомерные случайные величины.
30. Центральная предельная теорема.
31. Цепи Маркова.
32. Задача о линейном программировании.
33. Система массового обслуживания без очереди.
34. Система массового обслуживания с очередью.
35. Марковские процессы с дискретным временем, матрицы перехода дискретной цепи Маркова, предельные вероятности.
36. Метод Монте-Карло. Основные определения и понятия.
37. Генерирование значений дискретных случайных величин.
38. Генерирование траекторий случайных процессов.
39. Архитектура современных ЭВМ, принципы работы отдельных компонент.
40. Языки программирования высокого и низкого уровня, компиляторы и интерпретаторы.
41. Технология объектно-ориентированного программирования.
42. Операционные системы: функции ядра, функции защиты информации, основные типы ОС.

43. Локальные и глобальные вычислительные сети, типовые конфигурации, маршрутизация.
44. Основные протоколы обмена данными в вычислительных сетях, их информационная безопасность.
45. Системы управления базами данных, реляционная, иерархическая и сетевая модели, распределенные БД, защита информации в БД.
46. Теория сложности алгоритмов, классы сложности.
47. Деревья и графы, их представление в ЭВМ, обходы графов.
48. Алгоритмы на графах, выделение компонент связности.
49. Кратчайшие пути в графе, минимальный остов графа.
50. Деревья поиска и их применение.
51. Задача сортировки и основные алгоритмы сортировки.
52. Поиск информации методом хеширования.
53. Методы и средства привязки программ к аппаратному окружению и физическим носителям.
54. Методы и средства хранения ключевой информации в ЭВМ.
55. Защиты программ от изучения, защита от изменения и контроль целостности.
56. Защита от разрушающих программных воздействий.
57. История криптографии и ее основные достижения.
58. Шифры замены и перестановки, их свойства, композиции шифров.
59. Криптостойкость шифров, основные требования к шифрам.
60. Теоретическая стойкость шифров, совершенные и идеальные шифры.
61. Блоковые шифры.
62. Потоковые шифры.
63. Криптографические хеш-функции, их свойства и использование в криптографии.
64. Методы получения случайных последовательностей, их использование в криптографии.
65. Методы получения псевдослучайных последовательностей, их использование в криптографии.
66. Системы шифрования с открытыми ключами.
67. Криптографические протоколы.
68. Протоколы распределения ключей.
69. Протоколы идентификации.
70. Парольные системы разграничения доступа.
71. Цифровая подпись.
72. Стойкость систем с открытыми ключами. 1. Структура, классификация и основные характеристики технических каналов утечки информации.
73. Побочные электромагнитные излучения и наводки.
74. Классификация средств технической разведки, их возможности.
75. Концепция и методы инженерно-технической защиты информации.
76. Методы скрытия речевой информации в каналах связи.
77. Методы обнаружения и локализации закладных устройств.
78. Методы подавления опасных сигналов акустоэлектрических преобразователей.
79. Методы подавления информативных сигналов в цепях заземления и электропитания.
80. Виды контроля эффективности защиты информации.
81. Методы расчета и инструментального контроля показателей защиты информации.

Учебники и учебные пособия.

1. Имитационное моделирование: учебное пособие. Рекомендовано УМО вузов по университетскому политехническому образованию / Ю.Ю. Громов, Ю.С. Сербулов, И.Н. Корнфельд, В.О. Драчев, В.Г. Однолько. – Воронеж: ИПЦ «Научная книга», 2010.- 132 с.
2. Информационная безопасность и защита информации: учебное пособие. Рекомендовано УМО вузов по университетскому политехническому образованию/ Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова, Н.Г. Шахов - Старый Оскол: Изд-во Тонкие наукоёмкие технологии, 2010 г.-384с.
3. Информационная безопасность и защита информации: учебное пособие. Рекомендовано УМО вузов по университетскому политехническому образованию / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова, Н.Г. Шахов - Тамбов; М.; СПб; Баку; Вена: Изд-во «Нобелистика», 2009.- 128с.
4. Информационная безопасность и криптографические алгоритмы защиты информации: учебное пособие для проведения практических занятий. Рекомендовано УМО вузов по университетскому политехническому образованию / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова, Н.Г. Шахов, - Тамбов; М.; СПб; Баку; Вена: Изд-во «Нобелистика», 2009.- 76с.
5. Информационные технологии управления: учеб. пособие для вузов / под ред. проф. Г.А.Титоренко.– М.: ЮНИТИ-ДАНА, 2003.
6. Информационные технологии: учебное пособие. Рекомендовано УМО вузов по университетскому политехническому образованию / Ю.Ю. Громов, В.Е. Дидрих, И.В. Дидрих, В.Ф. Мартемьянов, В.О. Драчев, В.Г. Однолько - Тамбов; М.; СПб; Баку; Вена: Изд-во «Нобелистика», 2010.-130с.
7. Компьютерные телекоммуникации: учебное пособие. Рекомендовано УМО вузов по университетскому политехническому образованию / Ю.Ю. Громов, В.Е. Дидрих, И.В. Дидрих, Ю.Ф. Мартемьянов, В.О. Драчев, В.Г. Однолько. – Тамбов; М.; СПб; Баку; Вена: Изд-во «Нобелистика», 2010.- 198 с.
8. Лабораторный практикум по курсу «Основы теории управления»: учебное пособие. Рекомендовано УМО вузов по университетскому политехническому образованию / Ю.Ю. Громов, Ю.С. Сербулов, Н.Г. Шахов, Е.А. Шипилова, Ю.Ф. Мартемьянов, В.Г. Однолько. – Воронеж: ИПЦ «Научная книга», 2010. – 188 с.
9. Надежность информационных систем: учебное пособие. Рекомендовано УМО вузов по университетскому политехническому образованию / Ю.Ю. Громов, О.Г. Иванова, Н.Г. Мосягина, К.А. Набатов – Тамбов: Изд-во ГОУ ВПО ТГТУ, 2010.- 160 с.
10. Операционные системы. Концепции построения и обеспечения безопасности. Учебное пособие для вузов. Рекомендовано УМО вузов по университетскому политехническому образованию / Мартемьянов Ю. Ф., Яковлев Ал. В., Яковлев Ан. В.– М.: Горячая линия–Телеком, 2010. – 332 с.: ил
11. Основы теории управления: Учебное пособие. Рекомендовано УМО вузов по университетскому политехническому образованию / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова, Ю.С. Сербулов, К.А. Набатов. - Тамбов: Изд-во Тамб. гос. техн. ун-та, 2009. 240с.
12. Романов В.П. Интеллектуальные информационные системы в экономике: учеб. пособие / под ред. проф. Н.П. Тихомирова.– М.: Изд-во «Экзамен», 2003.
13. Теоретические основы передачи сигналов: учебное пособие: в 2 ч. ч.1. Рекомендовано УМО вузов по университетскому политехническому образованию / Ю.Ю. Громов, И.Г. Карпов, Г.Н. Нурутдинов, В.О. Драчев, В.Г. Однолько. – Тамбов: Изд-во МИНЦ «Нобелистика», 2010.-130с.
14. Теоретические основы передачи сигналов: учебное пособие: в 2 ч. ч.2. Рекомендовано УМО вузов по университетскому политехническому образованию / Ю.Ю. Громов, И.Г. Карпов, Г.Н. Нурутдинов, В.О. Драчев, В.Г. Однолько. – Тамбов: Изд-во МИНЦ «Нобелистика», 2010.-140с.
15. Теория информации и кодирования [Текст]: учеб. пособ. для вузов. Рекомендовано УМО вузов по университетскому политехническому образованию / Ю.Ю. Громов, В.О.

Драчев, О.Г. Иванова, Ю.С. Сербулов, АНОО ВИВТ, РосНОУ (ВФ). - Воронеж: Научная книга, 2009. - 177 с.
16. Управление данными: учебное пособие. Рекомендовано УМО вузов по университетскому политехническому образованию / Ю.Ю. Громов, О.Г. Иванова, В.Н. Точка. - Тамбов: Изд-во Тамб. гос. техн. ун-та, 2009. - 80с.
17. Численные методы в информационных системах: учебное пособие. Рекомендовано УМО вузов по университетскому политехническому образованию / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова, Ю.С. Сербулов, К.А. Набатов - Тамбов; М.; СПб; Баку; Вена: Изд-во «Нобелистика», 2009.-146с.

Периодические издания

1. Журнал «Безопасность информационных технологий»
2. Журнал «Вестник ВГУ. Серия системный анализ и информационные технологии»
3. Журнал «Вестник воронежского института ФСИН России»
4. Журнал «Инженерная физика»
5. Журнал «Информатика и ее применения»
6. Журнал «Информационно-измерительные и управляющие системы»
7. Журнал «Информационно-управляющие системы»
8. Журнал «Информационные технологии в проектировании и производстве»
9. Журнал «Информационные технологии и вычислительные системы»
10. Журнал «Информационные технологии»
11. Журнал «Информация и безопасность»

Программное обеспечение и Интернет-ресурсы

1. Библиотека научной литературы – www.lib.org.ru
2. Библиотека научных книг – www.bokod.narod.ru
3. Вестник ВГУ. Серия системный анализ и информационные технологии – www.vestnik.vsu.ru/content/analiz
4. Вестник Воронежского института ФСИН России – www.vifsinrf.ru
5. Сайт «Neuroschool» – www.neuroschool.narod.ru
6. Сайт «Компьютерные сети» – www.kompset.narod.ru
7. Сайт владикавказского математического журнала – www.vmj.ru
8. Сайт института математики им. С.Л. Соболева СО РАН – www.math.nsc.ru
9. Сайт института проблем информатики – www.ipian.kazan.ru
10. Сайт кафедры СИБ – www.kafedrasib.ru
11. Сайт основ физики и электротехники – www.fishelp.ru
12. Сайт факультета прикладной математики – www.fpm.miem.edu.ru
13. Сайт, посвященный параллельным вычислениям «x-com» – www.meta.parallel.ru
14. Электронная библиотека ИГЭУ – www.elib.ispu.ru/library