



МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное бюджетное государственное образовательное учреждение
высшего профессионального образования
«Тамбовский государственный технический университет»

УТВЕРЖДАЮ

И.о. ректора университета

М.Н. Краснянский

« 27 » марта 2015 г.

Вводится в действие с

« 30 » марта 2015 г.

ПРОГРАММА

вступительного экзамена в аспирантуру по специальной дисциплине

Направление подготовки 10.06.01 Информационная безопасность
(профиль подготовки 10.06.01.01 Методы и системы защиты информации,
информационная безопасность)

Форма обучения:

Очная, заочная

Составитель:

кафедра «Информационные системы и защита информации»

(наименование кафедры)


д.т.н., профессор Дидрих В.Е.

(ученая степень и звание, фамилия, инициалы составителя программы)

Тамбов 2015

СОГЛАСОВАНО

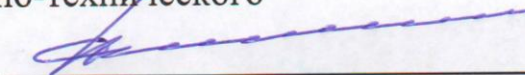
Начальник управления подготовки и
аттестации кадров высшей
квалификации ФГБОУ ВПО «ТГТУ»

 Е.И. Муратова
« 24 » марта 2015 г.

Программа вступительного экзамена в аспирантуру по направлению 10.06.01 Информационная безопасность разработана в соответствии с требованиями к уровню освоения выпускниками основных образовательных программ высшего образования (специалитет, магистратура) профессионального цикла дисциплин по направлению 10.05.03 Информационная безопасность автоматизированных систем (специалитет), 09.04.00 Информатика и вычислительная техника (магистратура).

Программа рассмотрена и утверждена на заседании Научно-технического совета университета протокол № 3 от « 26 » марта 2015 г.

Зам председателя Научно-технического
совета университета



С.И. Дворецкий

ПЕРЕЧЕНЬ ОБЩИХ ВОПРОСОВ ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ

10.06.01 Информационная безопасность

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 защиты интеллектуальной собственности.
10. Основы законодательства в области защиты информации.
11. Сочетания и размещения с повторениями, биномиальные коэффициенты, их свойства.
12. Алгебра логики, формулы алгебры логики, высказывания и операции, построение формул.
13. Булевы функции и формулы, функции алгебры логики, способы представления БФ, нормальные формы.
14. Случайные величины, математическое ожидание и дисперсия.
15. Основные законы распределения случайной величины.
16. Многомерные случайные величины.
17. Цепи Маркова.
18. Архитектура современных ЭВМ, принципы работы отдельных компонент.
19. Языки программирования высокого и низкого уровня, компиляторы и интерпретаторы.
20. Технология объектно-ориентированного программирования.
21. Операционные системы: функции ядра, функции защиты информации, основные типы ОС.
22. Локальные и глобальные вычислительные сети, типовые конфигурации, маршрутизация.
23. Основные протоколы обмена данными в вычислительных сетях, их информационная безопасность.
24. Системы управления базами данных, реляционная, иерархическая и сетевая модели, распределенные БД, защита информации в БД.
25. Теория сложности алгоритмов, классы сложности.
26. Деревья и графы, их представление в ЭВМ, обходы графов.
27. Деревья поиска и их применение.
28. Задача сортировки и основные алгоритмы сортировки.
29. Поиск информации методом хеширования.
30. История криптографии и ее основные достижения.
31. Криптостойкость шифров, основные требования к шифрам.
32. Теоретическая стойкость шифров, совершенные и идеальные шифры.
33. Побочные электромагнитные излучения и наводки.
34. Классификация средств технической разведки, их возможности.
35. Концепция и методы инженерно-технической защиты информации.

ПЕРЕЧЕНЬ ВОПРОСОВ ПО ПРОФИЛЮ ПОДГОТОВКИ

10.06.01.01 Методы и системы защиты информации, информационная безопасность

1. Методы решения систем линейных уравнений.
2. Методы численного решения дифференциальных уравнений.
3. Численные методы нахождения экстремумов функций.
4. Элементы комбинаторики: перестановки, выборки, сочетания и размещения без повторений.
5. Элементы теории графов: определение графа, способы представления.
6. Изоморфизм графов, элементы графов, валентность, маршруты, цепи, циклы.
7. Связность графов, подграфы, виды графов (тривиальные и полные; двудольные; планарные; направленные орграфы и сети) и операции над ними.
8. Теоремы сложения и умножения вероятностей.
9. Формула полной вероятности и Байеса.
10. Схема Бернулли, приближенные вычисления в схеме Бернулли.
11. Задача о линейном программировании.
12. Система массового обслуживания без очереди.
13. Система массового обслуживания с очередью.
14. Марковские процессы с дискретным временем, матрицы перехода дискретной цепи Маркова, предельные вероятности.
15. Метод Монте-Карло. Основные определения и понятия.
16. Генерирование значений дискретных случайных величин.
17. Генерирование траекторий случайных процессов.
18. Алгоритмы на графах, выделение компонент связности.
19. Кратчайшие пути в графе, минимальный остов графа.
20. Методы и средства привязки программ к аппаратному окружению и физическим носителям.
21. Методы и средства хранения ключевой информации в ЭВМ.
22. Защиты программ от изучения, защита от изменения и контроль целостности.
23. Защита от разрушающих программных воздействий.
24. Шифры замены и перестановки, их свойства, композиции шифров.
25. Блочные шифры.
26. Поточковые шифры.
27. Криптографические хеш-функции, их свойства и использование в криптографии.
28. Методы получения случайных последовательностей, их использование в криптографии.
29. Методы получения псевдослучайных последовательностей, их использование в криптографии.
30. Системы шифрования с открытыми ключами.
31. Криптографические протоколы.
32. Протоколы распределения ключей.
33. Протоколы идентификации.
34. Парольные системы разграничения доступа.
35. Цифровая подпись.
36. Стойкость систем с открытыми ключами. Структура, классификация и основные характеристики технических каналов утечки информации.
37. Методы скрытия речевой информации в каналах связи.
38. Методы обнаружения и локализации закладных устройств.
39. Методы подавления опасных сигналов акустоэлектрических преобразователей.
40. Методы подавления информативных сигналов в цепях заземления и электропитания.
41. Виды контроля эффективности защиты информации.
42. Методы расчета и инструментального контроля показателей защиты информации.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ

10.06.01 Информационная безопасность

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 ВИБТ, 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

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА ПО ПРОФИЛЮ ПОДГОТОВКИ

10.06.01.01 Методы и системы защиты информации, информационная безопасность

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 ВИБТ, 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