ФГБОУ ВО «ТГТУ» Прием 2017 Высшее образование Программы аспирантуры

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Тамбовский государственный технический университет»

ПРИНЯТО

решением Ученого совета ФГБОУ ВО «ТГТУ»
« 27 » марта 2017 г. (протокол № 3)

УТВЕРЖДЕНО

приказом ректора ФГБОУ ВО «ТГТУ»
« 29 » марта 2017 г. № 250-04

ПРОГРАММА
вступительного испытания для поступающих в 2017 году в аспирантуру
на направление подготовки
10.06.01 Информационная безопасность
по профилю
10.06.01.01 Методы и системы защиты информации, информационная безопасность

ПЕРЕЧЕНЬ 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. Блоковые шифры.
26. Потоковые 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

ФГБОУ ВО «ТГТУ» Прием 2017 Высшее образование Программы аспирантуры

СПИСОК ЛИТЕРАТУРЫ ДЛЯ ПОДГОТОВКИ К ВСТУПИТЕЛЬНЫМ ИСПЫТАНИЯМ

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ
10.06.01 Информационная безопасность

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 науко□мкие технологии, 2010. –384с.
3. 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.
4. 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.
5. 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.
6. Ю.Ю. Громов, О.Г. Иванова, Ю.Ф. Мартемьянов, Ю.К. Букурако, В.Г. Однолько. Методы организации защиты информации: учебное пособие (гриф Ученого совета ТГТУ). - Тамбов: Изд-во ФГБОУ ВПО «ТГТУ». – 2013. – 80 с.
7. Громов Ю.Ю., Гриднев В.А., Иванова О.Г., Поляков Д.В. Комплексное обеспечение информационной безопасности автоматизированных систем (курсовое и дипломное проектирование): учебное пособие (гриф Ученого совета ТГТУ). – Тамбов; М.; СПб.; Баку; Вена; Гамбург: Изд-во МИНЦ «Нобелистика». – 2012. – 80 с.
8. Громов Ю.Ю., Ивановский М.А., Дидрих В.Е., Иванова О.Г., Мартемьянов Ю.Ф., Старожилов О.Г. Методы анализа информационных систем. - Тамбов; М.; СПб.; Баку; Вена; Гамбург: Изд-во МИНЦ «Нобелистика». - 2012. – 220 с.
9. Информационная безопасность и защита информации: учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова, Н.Г. Шахов – 2-е изд., перераб. – Старый Оскол: ТНТ, 2015. – 384 с.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА ПО ПРОФИЛЮ ПОДГОТОВКИ
10.06.01.01 Методы и системы защиты информации, информационная безопасность

1. 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.
2. 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.
3. 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. – 130 с.
4. 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. – 140 с.
5. Громов Ю.Ю., Мартемьянов Ю.Ф., Яковлев А.В., Васюкова Е.О., Пеливан М.А. Операционные системы. Концепции построения и обеспечения безопасности: учебное пособие. – Тамбов: ФГБОУ ВПО «ТГТУ». – 2015.

Программа вступительных испытаний разработана кафедрой «Информационные системы и защита информации».