Федеральное государственное автономное образовательное учреждение высшего образования

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАДРЫ ВЫСШЕЙ КВАЛИФИКАЦИИ
(АСПИРАНТУРА)

УТВЕРЖДАЮ
Директор института
прикладной математики и
компьютерных наук
_____ С.П.Сущенко
« 14 » _____ 2018г.

ПРОГРАММА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ ПО СПЕЦИАЛЬНОЙ ДИСЦИПЛИНЕ
05.13.19 «Информационная безопасность»

Направление подготовки
10.06.01 - Информационная безопасность

Томск – 2018

Авторы – разработчики:
Доктор технических наук, профессор, профессор кафедры защиты информации и криптографии Геннадий Петрович Агибалов

Доктор физико-математических наук, доцент, заведующий кафедрой защиты информации и криптографии Николай Георгиевич Парватов

ПРОГРАММА РАССМОТРЕНА И ОДОБРЕНА на заседании учебно-методической комиссии института прикладной математики и компьютерных наук, протокол № 05 от «14» сентября 2018 года.

ОБЩИЕ ПОЛОЖЕНИЯ

Вступительное испытание по специальной дисциплине проводится в два этапа и в следующих формах:

Первый этап – экзаменационный по вопросам специальной дисциплины соответствующей направленности образовательной программы аспирантуры.

Второй этап – собеседование с руководителем основной образовательной программы аспирантуры по соответствующему направлению подготовки.

Для проведения собеседования поступающий предоставляет в отборочную комиссию до проведения вступительного испытания следующие документы:

- мотивационное письмо, в котором он обосновывает выбор направленности программы аспирантуры, выбор предполагаемого научного руководителя из числа преподавателей и научных работников университета, имеющих право осуществлять научное руководство аспирантами по соответствующей направленности образовательной программы аспирантуры (научной специальности), излагает профессиональные планы и цели подготовки и защиты кандидатской диссертации по выбранной научной специальности;

- рекомендательное письмо от предполагаемого научного руководителя с согласием осуществлять научное руководство в случае поступления на соответствующую программу аспирантуры. Рекомендательное письмо должно отражать наличие (или отсутствие) у поступающего:

- научного задела по теме предполагаемого диссертационного исследования;

- способностей и мотивации к проведению самостоятельных научных исследований.

Итоги каждого этапа вступительного испытания оформляются отдельным протоколом.

Этапы вступительного испытания по специальной дисциплине	**Максимальное количество баллов**
Первый этап (экзаменационный)	50
Второй этап (собеседование)	50

СОДЕРЖАНИЕ ВСТУПИТЕЛЬНОГО ЭКЗАМЕНА И ТЕМЫ ДЛЯ САМОСТОЯТЕЛЬНОЙ ПОДГОТОВКИ

Программа вступительного экзамена предназначена для поступающих в аспирантуру по профилю «Информационная безопасность» в качестве руководящего учебно-методического документа для целенаправленной подготовки к сдаче вступительного экзамена

Экзамен включает ключевые и практически значимые вопросы, относящиеся к следующим дисциплинам:

1. Алгебра
2. Дискретная математика
3. Методы программирования
4. Операционные системы
5. Компьютерные сети
6. Модели безопасности компьютерных систем
7. Защита в операционных системах
8. Криптографические методы защиты информации
9. Криптографические протоколы
10. Теоретико-числовые методы в криптографии
11. Алгоритмы кодирования и сжатия информации
12. Теория чисел.

Содержание экзамена охватывает следующие темы.

1. Алгебра. Темы для вступительного испытания.

1. Элементы теории множеств
2. Числовые системы, арифметика целых чисел и многочленов
3. Корни многочленов
4. Теория колец
5. Теория делимости в целостном кольце
6. Теория полей
7. Линейная алгебра
8. Теория групп

Перечень основной учебной литературы:

1. Глухов М., Елизаров В., Нечаев А. Алгебра. Лань. 2015. 608 с.
2. Кострикин А.И. Введение в алгебру. В 3х томах. Лань 2012.

Перечень дополнительной учебной литературы:

1. Фаддеев, Д.К. Лекции по алгебре. СПб. : Лань, 2007. 416 с.
2. Ленг С. Алгебра. Мир. 1968. 564 с.
3. Ван дер Варден. Алгебра. Мир. 1976. 648 с.
4. Прасолов В. В. Многочлены. МЦНМО 2001. 336 с.

2. Дискретная математика. Темы для вступительного испытания.

1. Разложение булевой функции по переменным, совершенные дизъюнктивная и конъюнктивная нормальные формы
2. Дизъюнктивная нормальная форма
3. Важнейшие замкнутые классы и функциональная полнота
4. Функции k-значной логики. Элементарные функции
5. Графы, их классификация и способы задания
6. Эйлеровы и гамильтоновы графы
7. Деревья. Остов минимального веса
8. Планарность. Формула Эйлера
9. Критерии планарности. Алгоритм укладки графа на плоскость
10. Раскраска графов. Оценки хроматического числа.
11. Раскраска планарных графов
12. Парасочетания
13. Ориентированные графы
14. Связность в орграфах. Отыскание сильных компонент
15. Построение матрицы достижимости. Алгоритм Уоршола
16. Сети. Алгоритм Форда-Фалкерсона

Перечень основной учебной литературы:

1. Яблонский С.В. Введение в дискретную математику. М.:Высшая школа. 2010. 381с.
2. Быкова С.В., Буркатовская Ю.Б. Булевы функции. Учебное пособие. Томск: ТГУ. 2008. 192 с.
3. Калугин Н.А., Калугин А.Н. Элементы теории графов. Самара: Изд-во СГАУ. 2013. 44 с.

Перечень дополнительной учебной литературы:

1. Конспект лекций О.Б.Лупанова по курсу «Введение в математическую логику» /Отв. ред. А.Б.Угольников. М.: Изд-во ЦПИ при механико-математическом факультете МГУ имени М.В.Ломоносова, 2007. – 192 с.

3. Методы программирования. Темы для вступительного испытания.

1. Этапы решения задачи коммивояжёра
2. Алгоритмы поиска подстроки в строке. БМ-поиск, КМП-поиск.
3. Простейшие алгоритмы сортировки
4. Алгоритм сортировки методом Хоара

5. Алгоритмы распределенной сортировки
6. Динамические списки
7. Алгоритмы топологической сортировки
8. Деревья как структура данных, работа с деревьями
9. АВЛ-деревья
10. Коды Хаффмана
11. Алгоритм Ху-Таккера кодирования информации
12. Оптимальное дерево поиска
13. Красно-черные деревья
14. B-деревья
15. Решение задачи коммивояжёра методом ветвей и границ

Перечень основной учебной литературы

1. Черёмушкин А.В. Лекции по арифметическим алгоритмам в криптографии. М.: МЦНМО, 2012.

2. Кормен Т., Лейзер Ч., Риверс Р.. АЛГОРИТМЫ: построение и анализ. М.: МЦНМО, 2010. 900 с.

Перечень дополнительной учебной литературы

3. Кнут Д. Искусство программирования для ЭВМ. В 3-х т. М.: Мир, 1978.

4. Страуструп Б. Язык программирования C++. М.: BINOM, 2000. 950 с.

4. Операционные системы. Темы для вступительного испытания.

1. Введение. Эволюция ОС. Классификация ОС. Архитектура ОС. Общая характеристика ОС; назначение и возможности систем клона UNIX. Основные компоненты ОС.
3. Режимы работы процессора. Реальный режим работы процессора. BIOS и UEFI. 4. Ассемблер процессора x86 в реальном режиме. Загрузчики ОС Linux: Grub, lilo.
5. Режимы работы процессора. Защищенный режим работы процессора. Механизмы защиты памяти. Сегментная и страничная организация памяти, виды адресов. GDT, LDT, переход в защищенный режим.
7. Виртуальная память. Принцип работы, реализация в процессорах x86. Алгоритмы замещения страниц. Динамические библиотеки, общая память, механизмы copy-on-write и zero-copy, отладка процессов.
8. Многозадачность и её виды. Алгоритмы планирования работы процессов при различных видах многозадачности.
9. Межпроцессное взаимодействие, примитивы межпроцессного взаимодействия. Сообщения, сокеты, общая память, пайпы, сигналы. Dbus, его функциональность и механизмы работы.
10. Примитивы синхронизации процессов. Мьютексы, семафоры. Способы реализации мьютексов. Алгоритм Петерсона. Задача «об обедающих философах». Задача «читателей и писателей». Задача «спящего брадобрея». События, мониторы, барьеры.
11. Управление памятью. Алгоритмы выделения памяти. Алгоритмы “best fit”, “first fit”, алгоритм близнецов. Выделение памяти в ядре, SLAB. Выделения памяти в прикладных процессах: dlmalloc, jemalloc. Принципы и основные моменты работы. Использование специфики алгоритмов при эксплуатации уязвимости переполнения буфера в куче.
12. Механизм прерываний процессора. Таблица векторов прерываний IDT в процессорах семейства x86. Обработка прерываний в защищенном режиме. Обработка прерываний с внешней аппаратуры. Чипы PIC 8259, APIC, их строение и принципы работы.
13. Файловые системы. Классическая ФС s5fs, организация дискового пространства, inode, жёсткие ссылки. Файловые системы ext2, ext3, ext4, fat, ntfs. Журналирование. Механизмы, предотвращающие фрагментацию.

Перечень основной учебной литературы

1. Столлингс В. Операционные системы. М.: Издательский дом «Вильямс», 2014. – 848 с.
2. Таненбаум Э. Современные операционные системы. СПб.: Питер, 2016. – 576 с.

Перечень дополнительной учебной литературы

1. Гордеев А.В. Операционные системы. СПб.: Питер, 2005. – 416 с.
2. Робачевский А.М. Операционная система UNIX. СПб.:BHV, 1999. – 528 с.

5. Компьютерные сети. Темы для вступительного испытания.
1. Принципы построения компьютерных сетей.
2. Технологии локальных вычислительных сетей.
3. Протоколы сетевого уровня.
4. Протоколы и технологии маршрутизации.
5. Протокол UDP.
6. Протокол TCP.
7. Система DNS.
8. Дизайн современных сетей.

Перечень основной учебной литературы
1. W. Richard Stevens, Kevin R. Fall. TCP/IP Illustrated, Volume 1: The Protocols (2nd edition), 2012. Addison Wesley.
2. У.Р. Стивенс, Б. Феннер, Э.М. Рудофф. UNIX: разработка сетевых приложений. 3-е изд. – СПб.: Питер, 2007. – 1039 с.

Перечень дополнительной литературы
3. Э. Немет, Г. Снайдер, Т. Хейн. Руководство администратора Linux.: Пер. с англ. – М. : Издательский дом “Вильямс”.
4. В.Г. Олифер, Н.А. Олифер. Компьютерные сети. – СПб.: Питер, 2004. – 864 с.

6. Модели безопасности компьютерных систем.
Темы для вступительного испытания.
1. Основные элементы и виды управления доступом.
2. Модели Грэхэм-Деннинг и Take-Grant.
3. Дискреционные ДП-модели.
4. Модели Белла-ЛаПадулы и Биба.
5. Мандатные ДП-модели.
6. Модель RBAC.
7. Ролевые ДП-модели.
8. Модель Харрисона-Руззо-Ульмана.
9. Паттерны формального моделирования управления доступом.
10. Разработка механизмов управления доступом для современных компьютерных систем

Перечень основной учебной литературы:
1. Девянин П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: Учеб. пособие для высш. учеб. заведений. – М.: Горячая Линия - Телеком, 2013. – 338 с.
2. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. М: Книжный мир, 2009. 352 с.
Перечень дополнительной учебной литературы:
1. Bishop M. Computer Security: art and science. - ISBN 0-201-44099-7, 2002. - 1084 p.
2. Девянин П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах. М.: Радио и связь, 2006. 176 с.

7. Защита в операционных системах.
Темы для вступительного испытания.
1. Введение в предмет. Аутентификация в ОС. Система PAM. Архитектура, принцип работы. Основные элементы файлов конфигурации PAM. Протокол аутентификации Kerberos.
2. Подсистемы ядра LSM и kauth. Архитектура, принцип работы, существующие модули. Примеры политик безопасности, реализованных с помощью LSM. Примеры политик безопасности, реализованных с помощью kauth.