МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ
Декан/Директор _____
«25» марта 2022 г.

ПРОГРАММА

вступительного испытания по специальной дисциплине
соответствующей научной специальности программы подготовки научных и научно-педагогических кадров в аспирантуре

2.3.6. Методы и системы защиты информации, информационная безопасность

Томск – 2022

Авторы-разработчики:

Замятин А.В., д-р техн. наук, профессор, директор института прикладной математики и компьютерных наук НИ ТГУ

Тренькаев В.Н., канд. техн. наук, доцент, доцент кафедры компьютерной безопасности НИ ТГУ

Вавилов В.А., канд. физ.-мат. наук, доцент, доцент кафедры программной инженерии НИ ТГУ

Согласовано:

Руководитель ОП  В.Н. Тренькаев

подпись

1. Общие положения

1.1. Программа вступительного испытания по специальной дисциплине соответствующей научной специальности программы подготовки научных и научно-педагогических кадров в аспирантуре 2.3.6. «Методы и системы защиты информации, информационная безопасность» (далее – Программа), сформирована на основе требований федеральных государственных образовательных стандартов высшего образования к программам магистратуры (специалитета) по соответствующим направлениям (специальностям) подготовки. Программа разработана для поступления на обучение в аспирантуру НИ ТГУ.

Программой устанавливается:

– форма, структура, процедура сдачи вступительного испытания;

– шкала оценивания;

– максимальное и минимальное количество баллов для успешного прохождения вступительного испытания;

– критерии оценки ответов.

Вступительное испытание проводится на русском языке или на английском языке для абитуриентов из стран дальнего зарубежья, поступающих на обучение по PhD программе.

Форма, процедура сдачи вступительного испытания, а также шкала оценивания и критерии оценки ответов экзаменуемого, установленные Программой, не зависят от языка проведения вступительного испытания.

1.2. Организация и проведение вступительного испытания осуществляется в соответствии с Правилами приема, утвержденными приказом ректора НИ ТГУ, действующими на текущий год поступления.

1.3. По результатам вступительного испытания, поступающий имеет право подать на апелляцию о нарушении, по мнению поступающего, установленного порядка проведения вступительного испытания и (или) о несогласии с полученной оценкой результатов вступительного испытания в порядке, установленном Правилами приема, действующими на текущий год поступления.

2. Форма, структура, процедура, программа вступительного испытания и шкала оценивания ответов

2.1. Вступительное испытание по специальной дисциплине проводится в форме экзамена письменно в соответствии с перечнем тем и (или) вопросов, установленных данной Программой.

Структура экзамена:

Экзамен проводится по экзаменационным билетам, включающим два вопроса. При формировании билета вопросы случайным образом берутся из двух различных разделов.

2.2. Процедура проведения экзамена представляет собой сдачу экзамена в очной форме и (или) с использованием дистанционных технологий (при условии идентификации поступающих при сдаче ими вступительных испытаний):

1) очно и дистанционно; 2) только дистанционно; 3) только очно.

Для дистанционной формы проведения экзамена используются платформы Moodle и программы для организации видеоконференций: Zoom , Adobe Connect и другие. Для наблюдения за участниками экзамена и идентификации их личности создана система прокторинга. Проктор (наблюдатель) перед началом экзамена при помощи веб-камеры абитуриента проводит инструктаж и собеседование по вопросам организации и проведения экзамена, идентификацию личности путем сравнивания фото в паспорте и лица сдающего (абитуриент показывает в веб-камеру свой паспорт в развернутом виде рядом со своим лицом).

Видео, транслируемое с веб-камеры участника экзамена, доступно проктору для наблюдения и записывается на сервер для дальнейшего просмотра при возникновении спорных ситуаций.

2.3. Результаты проведения вступительного испытания оформляются протоколом, в котором фиксируются вопросы экзаменаторов к поступающему. На каждого поступающего ведется отдельный протокол.

2.4. Программа экзамена.

Экзамен проводится по экзаменационным билетам, включающим два вопроса. При формировании билета вопросы случайным образом берутся из двух различных разделов.

1. АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

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

Перечень основной учебной литературы:

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

Перечень дополнительной учебной литературы:

1. Ван дер Варден. Алгебра. – М.: Мир, 1976. – 648 с.
2. Ларин С. В. Алгебра и теория чисел. Группы, кольца и поля: Учебное пособие для вузов. – М.: Юрайт, 2022. – 160 с.
3. Ленг С. Алгебра. – М.: Мир, 1968. – 564 с.
4. Мартынов Л. М. Алгебра и теория чисел для криптографии. – СПб.: Лань, 2022. – 456 с.
5. Платонов В. П. Алгебраические группы и теория чисел. – М.: Наука, 1991. – 654 с.
6. Прасолов В. В. Многочлены. – МЦНМО, 2001. – 336 с.
7. Фаддеев Д.К. Лекции по алгебре. – СПб.: Лань, 2007. – 416 с.

2. ДИСКРЕТНАЯ МАТЕМАТИКА

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. – 381 с.
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 ММФ МГУ им. М.В.Ломоносова, 2007. – 192 с.

2. Гашков С.Б. Дискретная математика. Учебник для вузов. – СПб.: Лань, 2022. – 456 с.

3. Кудрявцев В.Б. Дискретная математика. Теория однородных структур: Учебник для вузов / Кудрявцев В.Б., Подколзин А.С., Болотов А.А. – М.: Юрайт, 2022. – 295 с.

3. МЕТОДЫ ПРОГРАММИРОВАНИЯ

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

1. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. – М.: Мир, 1979.

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

3. Костюк Ю.Л. Основы программирования. Разработка и анализ алгоритмов. – Томск: Изд-во Том. ун-та, 2006. – 244 с.

4. Кристофидес Н. Теория графов. Алгоритмический подход. – М.: Мир, 1978.

5. Малявко А. А. Формальные языки и компиляторы: Учебное пособие для вузов. – М.: Юрайт, 2022. – 429 с.

6. Огнева М. В. Программирование на языке С++: практический курс : Учебное пособие для вузов / Огнева М. В., Кудрина Е. В. – Москва : Юрайт, 2022. – 335 с.

7. Страуструп Б. Язык программирования С++. – М.: BINOM, 2000. – 950 с.

4. ОПЕРАЦИОННЫЕ СИСТЕМЫ

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.: 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. Гостев И. М. Операционные системы : Учебник и практикум для вузов. – М.: Юрайт, 2022. – 164 с.

3. Замятин А. В., Сущенко С.П. Операционные системы: учебное пособие. – Томск: Изд-во Том. ун-та, 2020. – 220 с.

4. Кобылянский В. Г. Операционные системы, среды и оболочки. – СПб.: Лань, 2021. – 120 с.

5. Робачевский А.М. Операционная система UNIX. – СПб.: BHV, 1999. – 528 с.

5. КОМПЬЮТЕРНЫЕ СЕТИ

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. Stevens W. Richard, Kevin R. Fall. TCP/IP Illustrated. Vol. 1: The Protocols (2-nd edition), 2012.

2. Стивенс У.Р., Б. Феннер, Э.М. Рудофф. UNIX: разработка сетевых приложений. 3-е изд. – СПб.: Питер, 2007. – 1039 с.

Перечень дополнительной литературы

1. Дибров М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1. Учебник и практикум. – М.: Юрайт, 2022. – 333 с.

2. Замятина О. М. Инфокоммуникационные системы и сети. Основы моделирования: Учебное пособие. – М.: Юрайт, 2022. – 159 с.

3. Нефедов В. И. Общая теория связи : Учебник для вузов / Нефедов В. И., Сигов А. С. ; под ред. Нефедова В.И. – М.: Юрайт, 2022. – 495 с.

4. Олифер В.Г., Олифер Н.А. Компьютерные сети. – СПб.: Питер, 2004. – 864 с.

5. Скляров О. К. Волоконно-оптические сети и системы связи. – СПб.: Лань, 2022. – 268 с.
6. Танненбаум Э. Компьютерные сети. – СПб.: Питер, 2002. – 848 с.

6. МОДЕЛИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ.

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 вузов. – 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. Богульская Н. Модели безопасности компьютерных систем: Учебное пособие. – Красноярск: СФУ, 2019. – 206 с.
3. Грушо А. А. Теоретические основы компьютерной безопасности. / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. – М.: Академия, 2009. – 267 с.
4. Девянин П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах. – М.: Радио и связь, 2006. – 176 с.

7. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

1. Основные понятия и задачи криптографии
2. Шифры замены и перестановки
3. Симметричные схемы шифрования
4. Асимметричное шифрование
5. Электронная цифровая подпись

6. Криптографический функции хэширования

7. Криптографические протоколы

Перечень основной учебной литературы:

1. Запечников С. В. Криптографические методы защиты информации: Учебник для вузов / Запечников С. В., Казарин О. В., Тарасов А. А. – М.: Юрайт, 2022. – 309 с.

2. Математические и компьютерные основы криптологии / Ю. С. Харин, В. И. Берник, Г. В. Матвеев, С. В. Агиевич. – Минск: Новое знание, 2003. – 381 с.

3. Стохастические методы и средства защиты информации в компьютерных системах и сетях / Иванов М. А., Ковалев А. В., Мацук Н. А. [и др.] ; под ред. Жукова И. Ю. – М.: КУДИЦ-Пресс, 2009. – 510 с.

Перечень дополнительной учебной литературы:

1. Бабаш А. В. История защиты информации в зарубежных странах: учебное пособие: [для студентов вузов по направлению информационной безопасности и прикладной информатики] / А. В. Бабаш, Д. А. Ларин. – М.: РИОР [и др.], 2013. – 283 с.

2. Баранова Е. К. Криптографические методы защиты информации: лабораторный практикум / Е. К. Баранова, А. В. Бабаш. – М.: Кнорус, 2015. – 196 с.

3. Васильева И. Н. Криптографические методы защиты информации : учебник и практикум. – М.: Юрайт, 2016. – 348 с.

4. Зубов А. Ю. Криптографические методы защиты информации. Совершенные шифры: [учебное пособие для студентов вузов по специальностям "Информационная безопасность"] – М.: Гелиос АРВ, 2005. – 190 с.

5. Технические средства и методы защиты информации : [учебное пособие для студентов вузов, обучающихся по специальностям 090102 – "Компьютерная безопасность", 090105 - "Комплексное обеспечение информационной безопасности автоматизированных систем", 090106 - "Информационная безопасность телекоммуникационных систем"] / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков [и др.] ; под ред. А. П. Зайцева, А. А. Шелупанова. – М.: Горячая линия – Телеком, 2009. – 614 с.

6. Фомичёв В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : Учебник для вузов / Фомичёв В. М., Мельников Д. А. ; под ред. Фомичёва В.М. – М.: Юрайт, 2022. – 209 с.

7. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. – М.: ДМК Пресс, 2012. – 592 с.

8. ТЕОРИЯ ИНФОРМАЦИИ И КОДИРОВАНИЕ

1. Коды, информация, энтропия, избыточность, кодирование Хаффмана.

2. Помехоустойчивое кодирование. Коды Хемминга

3. Датчики случайных величин. Последовательность Лемера

4. Алгоритмы над сверхдлинными числами

5. Представление и методы преобразования цифрового видео

6. Алгоритмы сжатия данных. Энтропийные методы

7. Сжатие изображений и видео

8.Алгоритмы кодирования изображений: JPEG, JPEG2000

9. Стандарты кодирования цифрового видео: H.261, MPEG1, MPEG2, MPEG4, H.265/AVC

10. Стандарты кодирования звуковых сигналов: MPEG1 Audio, MPEG2 Audio, AC-3

11. Форматы передачи данных по сетям: стандарты кодирования MPEG2 TS, OGG, MP4, WMS

12. Передача данных на постоянных носителях: стандарты кодирования MPEG2 PS, OGG, AVI, WMA/WMV

Перечень основной учебной литературы:

1. Голиков А. М. Модуляция, кодирование и моделирование в телекоммуникационных системах. Теория и практика. – СПб.: Лань, 2022. – 452 с.

2. Осокин А. Н. Теория информации: Учебное пособие для вузов / Осокин А. Н., Мальчуков А. Н. – М.: Юрайт, 2022. – 205 с.

Перечень дополнительной учебной литературы:

1. Ахо А., Ульман Дж. Теория синтаксического анализа, перевода и компиляции. Т. 1. Синтаксический анализ. – М.: Мир, 1978.

2. Волкова В. Н. Теория информационных процессов и систем : Учебник и практикум для вузов. – М.: Юрайт, 2022. – 432 с.

3. Кульбак С. Теория информации и статистика / Пер. с англ. Д. И. Гордеева и А. В. Прохорова; Под ред. и с предисл. А. Н. Колмогорова. – М.: Наука, 1967. – 408 с.

4. Матвеев Б. В. Основы корректирующего кодирования: теория и лабораторный практикум. – СПб.: Лань, 2021. – 192 с.

5. Методы компьютерной обработки изображений: [Учебное пособие для студентов по специальности "Прикладная математика"] / Гашников М. В. , Глумов Н. И. , Ильясова Н. Ю. и др. ; Под ред. В. А. Сойфера. – М.: Физматлит, 2001. – 780 с.

6. Нефедов В. И. Общая теория связи: Учебник для вузов / Нефедов В. И., Сигов А. С. ; под ред. Нефедова В.И. – М.: Юрайт, 2022. – 495 с.

2.5. Шкала оценивания ответов на экзамене:

неудовлетворительно	**удовлетворительно**	**хорошо**	**отлично**
до 59 баллов	60 – 75 баллов	76 – 84 баллов	85 – 100 баллов

Общая продолжительность экзамена составляет 45 минут.

Максимальное количество баллов за экзамен – 100. Минимальное количество баллов для успешного прохождения экзамена – 60. Поступающий, набравший менее 60 баллов за экзамен, не может быть зачислен в аспирантуру.

Таблица критериев оценки устных и письменных ответов (при наличии)

Вид деятельности		
Оценка	Балл	Уровень владения темой
неудовлетворительно	до 59	Выставляется абитуриенту, который не продемонстрировал значительной части материала, допускает существенные ошибки, показывает фрагментарные знания (или их отсутствие), частично освоенное умение (или его отсутствие). Списывание является основанием для получения оценки «неудовлетворительно».
удовлетворительно	60-75	Выставляется абитуриенту, который имеет знания только основного материала, но не усвоил его детали, допускает неточности, недостаточно правильные формулировки, нарушения последовательности в изложении материала. Показывает общее, но не структурированное знание, в целом успешное, но не систематическое умение.
хорошо	76-84	Выставляется абитуриенту, который твердо знает материал, грамотно и по существу его излагает. Не допускает существенных неточностей в ответе на вопросы. Соответствующие знания и умения в целом сформированы, но содержат отдельные пробелы.
отлично	85-100	Выставляется абитуриенту, который глубоко и прочно усвоил материал и исчерпывающе, грамотно, логически стройно и творчески его изложил. Соответствующие знания и умения сформированы полностью.

Вступительное испытание проводится экзаменационной комиссией, действующей на основании приказа ректора.

Итоговая оценка за экзамен определяется как средний балл, выставленный всеми членами экзаменационной комиссии.