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_____
«19» октября 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:

Тренькаев В.Н., канд. техн. наук, доцент, доцент кафедры компьютерной безопасности 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 виде экзамена в соответствии с перечнем тем и (или) вопросов, установленных данной Программой, в устной форме, при этом, рекомендуется основные моменты ответа фиксировать в письменном виде.

Структура экзамена:

Экзамен проводиться в виде собеседования с целью выявления у абитуриента объема научных знаний, научно-исследовательских компетенций, навыков системного и критического мышления, необходимых для обучения в аспирантуре. Абитуриент должен показать профессиональное владение теорией и практикой в предметной области, продемонстрировать умение вести научную дискуссию. Вступительное испытание состоит из ответов на вопросы билета и дополнительные вопросы в рамках программы экзамена.

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
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. – СПб.: Лань, 2015. – 608 с.

2. Кострикин А.И. Введение в алгебру. В 3-х томах. – СПб.: Лань, 2012.

Перечень дополнительной учебной литературы:

1. Ларин С. В. Алгебра и теория чисел. Группы, кольца и поля: Учебное пособие для вузов. – М.: Юрайт, 2022. – 160 с.

2. Ленг С. Алгебра. – М.: Мир, 1968. – 564 с.

3. Мартынов Л. М. Алгебра и теория чисел для криптографии. – СПб.: Лань, 2022. – 456 с.

4. Платонов В. П. Алгебраические группы и теория чисел. – М.: Наука, 1991. – 654 с.

5. Прасолов В. В. Многочлены. – МЦНМО, 2001. – 336 с.

6. Фаддеев Д.К. Лекции по алгебре. – СПб.: Лань, 2007. – 416 с.

2. ДИСКРЕТНАЯ МАТЕМАТИКА

1. Разложение булевой функции по переменным
2. Дизъюнктивная (конъюнктивная) нормальные формы
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. Критерии планарности
9. Раскраска графов. Оценки хроматического числа.
10. Раскраска планарных графов
11. Ориентированные графы
12. Связность в орграфах. Отыскание сильных компонент

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. АЛГОРИТМЫ И СТРУКТУПЫ ДАННЫХ

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

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

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

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

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

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

4. ОПЕРАЦИОННЫЕ СИСТЕМЫ

1. Эволюция ОС. Классификация ОС.
2. Архитектура ОС. Общая характеристика ОС.
3. Режимы работы процессора.
4. Ассемблер процессора x86 в реальном режиме.

5. Виртуальная память.
6. Многозадачность и её виды.
7. Межпроцессное взаимодействие.
8. Примитивы синхронизации процессов.
9. Управление памятью. Алгоритмы выделения памяти.
10. Механизм прерываний процессора.
11. Файловые системы.

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. Немет Э., Снайдер Г., Хейн Т. Unix и Linux. Руководство администратора. – М.: Вильямс, 2020. – 1168 с.

4. Нефедов В. И., Сигов А. С. Общая теория связи : Учебник для вузов. – М.: Юрайт, 2022. – 495 с.

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

6. Скляров О. К. Волоконно-оптические сети и системы связи. – СПб.: Лань, 2022. – 268 с.

7. Танненбаум Э. Компьютерные сети. – СПб.: Питер, 2002. – 848 с.

6. БАЗЫ ДАННЫХ

1. Общие принципы построения баз данных.
2. Модели данных.
3. Проектирование баз данных.
4. Язык запросов SQL.
5. Системы управления базами данных (СУБД).
6. Нереляционные СУБД (NoSQL).
7. Распределенные базы данных.

Перечень основной учебной литературы:

1. Грофф Д. и др. SQL. Полное руководство. – М.: Диалектика, 2019.

2. Кукарцев В.В. Теория баз данных: учебник.– Красноярск: Сибирский федеральный университет, 2017.

Перечень дополнительной учебной литературы:

1. Голицына О.Л. Базы данных: учебное пособие. – М.: Форум, 2020.

2. Дейт К. Дж. Введение в системы баз данных. 8-е изд.: пер. с англ. – М.: Вильямс, 2008. – 1328 с.

7. 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. Механизмы 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.

8. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

1. Основные понятия и задачи криптографии
2. Методы криптоанализа (линейный, дифференциальный)
3. Модель шифра по К.Шеннону
4. Блочные шифры (Магма, Кузнечик, AES)
5. Стойкие генераторы псевдослучайных чисел
7. Ассиметричные шифры (RSA, шифр Эль-Гамаля)
8. Цифровая подпись. Инфраструктура открытых ключей
9. Криптографические функции хеширования (Стрибог, SHA-3)

Перечень основной учебной литературы:

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. Учебное пособие. – М.: Гелиос АРВ, 2002.– 480 с.

2. Бабаш А.В. Криптографические методы защиты информации. – М.: Изд. Центр РИОР, 2019.– 413 с.

3. Кузьминов Т.В. Криптографические методы защиты информации / Т.В. Кузьминов. – Новосибирск: Наука, 1998. – 194 с.

4. Лось А.Б. Криптографические методы защиты информации: учебник для академического бакалавриата / Лось А. Б., Нестеренко А. Ю., Рожков М. И. – М: Юрайт, 2018.

Перечень дополнительной учебной литературы:

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

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

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

4. 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.

5. 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.

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

9. КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

1. Классификация протоколов
2. Виды атак на протоколы
2. Протоколы аутентификации сообщений
4. Протоколы идентификации
5. Протоколы с нулевым разглашением
7. Протоколы распределения ключей (Kerberos)
8. Протоколы открытого распределения ключей
9. Протоколы предварительного распределения ключей
10. Групповые криптографические протоколы
11. Прикладные криптографические протоколы (IPsec, SSL/TLS)

Перечень основной учебной литературы:

1. Мао Венбо Современная криптография: теория и практика. – М.: Вильямс, 2005. – 768 с.

2. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. – М.: Академия, 2009. – 271 с.

Перечень дополнительной учебной литературы:

1. Запечников С.В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности: учеб. пособие. – М.: Горячая линия – Телеком, 2006. – 319 с.

2. Шнайер Б. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – 816 с.

10. ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

1. Защита от атак канального уровня
2. Защита коммутации.
2. Технология VPN

4. Защита от атак DoS и DDoS
5. Защита маршрутизации
7. Защита транспортного уровня
8. Защита сетевых устройств
9. Технологии межсетевого экранирования
10. Методы и технологии обнаружения вторжений
11. Сканирование защищенности сетей

Перечень основной учебной литературы:

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

Перечень дополнительной учебной литературы:

1. Stevens W. R., Fall K.R. TCP/IP Illustrated. Vol.1: The Protocols, 2012.
2. Convery S. Network Security Architectures // Cisco Press, 2011. – 792 p.

11. ЗАЩИТА В ОПЕРАЦИОННЫХ СИСТЕМАХ

1. Понятие защищенной ОС
2. Управление доступом
3. Идентификация, аутентификация и авторизация
4. Аудит. Политика аудита. Реализация аудита
5. Интеграция защищенных ОС в защищенную сеть

Перечень основной учебной литературы:

1. Проскурин В.Г. Защита в операционных системах. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2014. – 192 с.
2. Буренин П.В. и др. Безопасность операционной системы специального назначения Astra Linux Special Edition. – М.: Горячая линия – Телеком, 2019. – 404 с.

Перечень дополнительной учебной литературы:

1. Шаньгин В. Комплексная защита информации в корпоративных системах: Учебное пособие. – М.: Форум, 2018. – 592 с.

12. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Информационная безопасность в системе национальной безопасности РФ
2. Основные термины и определения в области информационной безопасности
3. Классификация уязвимостей и угроз. Базы данных уязвимостей
4. Классификация и характеристика методов и средств защиты информации
5. Международные стандарты в области информационной безопасности
6. Нормативно-правовая база РФ в области информационной безопасности
7. Нормативно-технические документы РФ в области обеспечения информационной безопасности

8. Система сертификации средств защиты информации в РФ
9. Лицензирование деятельности в области защиты информации в РФ
10. Управление информационной безопасностью
11. Политика информационной безопасности организации

Перечень основной учебной литературы:

1. Нестеров С.А. Основы информационной безопасности: учебное пособие. 5-е изд., стер. – СПб.: Лань, 2019. – 324 с.
2. Баранова Е.К., Бабаш А.В. Основы информационной безопасности: учебник. – М.: РИОР, ИНФРА-М, 2019. – 202 с.

Перечень дополнительной учебной литературы:

1. Галатенко В. А. Основы информационной безопасности: учебное пособие. 4-е изд. – М.: Интернет-Университет ИТ, 2010. – 205 с.
2. Белов Е.Б. Основы информационной безопасности: учебное пособие / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – М.: Горячая линия - Телеком, 2006. – 544 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.