

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»
Физико-технический факультет**

УТВЕРЖДЕНО:

на заседании Ученого совета
физико-технического факультета
протокол № 6 от 15.02.2019 г.
председатель совета

С.А. Фоменко



ПРОГРАММА

профильного экзамена по специальности
для абитуриентов, поступающих на обучение
по образовательной программе

МАГИСТРАТУРЫ

на направление подготовки

10.04.01 Информационная безопасность

Донецк, 2019

Содержание программы

1. Введение	3
2. Общие положения	4
3. Перечень вопросов для подготовки к сдаче вступительного испытания и список рекомендованной литературы	5
4. Структура билета	13
5. Образец бланка ответов	14
6. Критерии оценивания письменных ответов на вступительном испытании	15

1. Введение

Целью вступительного испытания в магистратуру по направлению подготовки 10.04.01 Информационная безопасность является проверка теоретической и практической подготовки абитуриентов для освоения программы магистратуры, а также для прохождения конкурса.

Требования к уровню подготовки абитуриентов. Для успешного освоения образовательной программы магистратуры абитуриенты должны иметь квалификацию бакалавр с направлением подготовки 10.03.01 Информационная безопасность, решать теоретические и практические задания в рамках программы бакалавриата.

Характеристика содержания программы. Вступительное испытание имеет междисциплинарный комплексный характер. Программа вступительного испытания основывается на разделах следующих учебных дисциплин:

1. Высшая математика;
2. Теория вероятности;
3. Физика;
4. Электроника;
5. Основы теории цепей, сигналы и процессы в электронике;
6. Информационные технологии;
7. Технологии программирования;
8. Архитектура компьютерных систем;
9. Объектно-ориентированное программирование;
10. Теория информации и кодирования;
11. Комплексные системы защиты информации: проектирование, внедрение, сопровождение;
12. Прикладная криптология;
13. Информационно-коммуникационные системы;
14. Защита информации в информационно-коммуникационных системах;
15. Системы технической защиты информации;
16. Цифровая обработка сигналов;
17. Системы цифровой обработки сигналов,

теоретические и практические аспекты в которых, позволяют успешно выполнить задания на вступительном испытании.

Порядок проведения вступительного испытания определяется Положением о приемной комиссии ГОУ ВПО «Донецкий национальный университет».

2. Общие положения

Для обучения по образовательной программе магистратуры по направлению подготовки 10.04.01 Информационная безопасность принимаются абитуриенты, имеющие квалификацию бакалавр с направлениями подготовки 10.03.01 Информационная безопасность.

Программа вступительного испытания содержит вопросы из фундаментальных и профессионально-ориентированных дисциплин.

С целью повышения значимости фундаментальных дисциплин при подготовке будущих квалифицированных специалистов, улучшения их общего профессионального уровня, конкурентоспособности на рынке труда и быстрой адаптации в условиях современного научно-технического прогресса в программу вступительного испытания включён ряд вопросов из различных разделов математики, общей и теоретической физики.

Вступительное испытание проводится в форме письменного экзамена по билетам, содержащих 2 задания: оценка за выполнение первого задания 60 баллов, оценка за выполнение второго задания – 40 баллов. Максимальное количество баллов за решение всех заданий 100 баллов. Продолжительность письменного экзамена – два астрономических часа (120 минут). Отсчет времени начинается после заполнения титульного листа ответов. При выполнении заданий поступающим запрещается пользоваться учебниками, мобильными телефонами и другими устройствами, предназначенными для хранения, приема и передачи информации. Разрешается использование калькуляторов.

3. Перечень вопросов для подготовки к сдаче вступительного испытания и список рекомендованной литературы

Высшая математика

1. Числовые последовательности. Предел.
2. Функции одной переменной. Предел, непрерывность, дифференцируемость.
3. Функции многих переменных. Предел, непрерывность, дифференцируемость.
4. Интегралы: неопределенный, определенный, кратные, криволинейные, несобственные.
5. Великие формулы математического анализа: Ньютона-Лейбница, Грина, Остроградского, Стокса.
6. Ряды: числовые степенные, Фурье.
7. Преобразования Лапласа и Фурье.
8. Дифференциальные уравнения первого порядка, линейные n -го порядка. Метод вариации постоянных.
9. Уравнения в частных производных. Метод Фурье.
10. Кривые второго порядка. Билинейные, квадратические формы. Матрицы, определители. Теорема Кронекера-Капелли.

Литература:

1. Анго А. Математика для электро- и радиоинженеров. Москва. Наука. 1965.
2. Фихтенгольц Г.М. Основы математического анализа. 2005.
2. Запорожец Г.И. Руководство к решению задач по математическому анализу. Издание четвертое. Москва. Высшая школа. 1966.
3. Д.Г. Орловский. Неопределенный интеграл. Практикум. СПб. «Лань». 2006.
4. Двайт Г.Б. Таблицы интегралов и другие математические формулы. Пер. с англ. Н.В. Леви. СПб. «Москва». 2005.
5. Залманзон Л.А. Преобразования Фурье, Уолша, Хаара и их применение в управлении, связи и других областях. Москва. Наука. 1989.
6. Бронштейн И.С., Семендяев К.А. Справочник по математике для инженеров и учащихся втузов. – М. – Наука. – 1981.

Теория вероятности

1. Теорема сложения и умножения вероятностей. Формула полной вероятности. Формула Байеса.
2. Дискретная случайная величина. Законы распределения. Функция распределения случайной величины и ее свойства.
3. Биноминальное распределение случайной величины. Математическое ожидание. Дисперсия. Среднее квадр. отклонение.

4. Нормальный закон распределение случайной величины. Математическое ожидание. Дисперсия. Среднее квадр. отклонение.
5. Понятие о генеральной совокупности и выборке. Выборочная средняя, выборочная дисперсия, выборочная среднеквадратическое отклонение.

Литература:

1. Гмурман В.Е. Теория вероятностей и математическая статистика.
2. Гмурман В.Е. Руководство к решению задач по теории вероятности и математической статистики.
3. Кремер Н.Ш.. Теория вероятностей и математическая статистика.

Физика

1. Закон Кулона. Потенциал и напряженность поля диполя. Электрическая индукция в проводнике. Опыты Фарадея по электромагнитной индукции. Закон индукции.
2. Закон Ома в дифференциальной форме.
3. Резонаторы в цепях переменного тока. Резонанс токов и напряжений. Работа и мощность переменного тока.
4. Система уравнений Максвелла для электромагнитного поля (смысл, содержание). Материальные уравнения.
5. Волновое уравнение. Решение волнового уравнения в общем виде для одномерного случая.
6. Поглощение света. Коэффициент поглощения. Фазовая и групповая скорости. Формула Рэлея.
7. Формула Планка. Кванты света. Фотоэффект. Дуализм электромагнитного излучения.
8. Интерференция двух монохроматических волн. Временная и пространственная когерентность.
9. Оптический квантовый генератор. Инверсная заселенность. Генерация излучения. Устройство гелий-неонового лазера.

Литература:

1. Иродов И.Е. Основные законы электромагнетизма.- М.: Высш. шк., 1983.-279 с.
2. Савельев И.В. Общий курс физики. Т.2, Т.3.- М.: Наука, 1970. - 431 с.
3. Матвеев А.Н. Электричество и магнетизм.- М.: Высш. шк.. 1983.- 463 с.
4. Сивухин Д.В. Общий курс физики. Электричество. Оптика.- М.: Наука, 1980. - 752с.
5. Калашников С.Г. Электричество. – М.: Наука, 1977. – 560 с.
6. Матвеев А.Н. Оптика.- М.: Высш. шк., 1985.- 351 с.
7. Ландсберг Г.С. Общий курс физики. Оптика.- М.: Наука, 1976. - 928 с.
8. Бутиков Е.И. Оптика.- Спб: Невский диалект; 2003. – 480 с.

Электроника

1. Принципы функционирования полупроводниковых приборов. Полупроводниковые диоды.
2. Полупроводниковые датчики и индикаторные приборы. Приборы с зарядовой связью.
3. Последовательностные логические устройства. Одноступенчатые триггеры.

Литература:

1. Опадчий Ю.Ф., Глудкин О.П., Гуров А.И. Аналоговая и цифровая электроника. Москва. Горячая линия. 1999.
2. Гутников В.С. Интегральная электроника в измерительных устройствах. Ленинград. Энергия. 1980.
3. Жеребцов М.П. Введение в электронику. Москва. Энергия. 1960.

Основы теории цепей, сигналы и процессы в электронике

1. Классификация сигналов.
2. Оптимальная фильтрация сигналов на фоне помех. Импульсная характеристика согласованного фильтра.
3. Основные элементы радиоэлектронных цепей. Классификация цепей.

Литература:

1. Гимпилевич Ю.Б. Сигналы и процессы в радиотехнике. Севастополь. 2003.
2. Каяцкас А.Я. Основы радиоэлектроники
3. Попов. Основы теории цепей. Москва. Высшая школа. 1985.

Технологии программирования

1. Жизненный цикл разработки программного обеспечения
2. Типы данных, переменные, алгоритмы, представление основных структур программирования.
3. Процедуры и функции как модульное программирование.
4. Технологии и методы программирования.

Литература:

1. Вельбицкий, И. В. Технология программирования. - Киев: Техніка, 1984. - 279 с.
2. Терехов, А. Н. Технология программирования: учеб. пособие по специальности "Мат. обеспечение и администрирование информ. систем" М.: Интернет-Ун-т Информ. Технологий: БИНОМ. Лаб. знаний, 2007. - 148 с.

Информационные технологии

1. Общее понятие об информационных технологиях. Информация и информационные процессы (передача, получение, обработка, защита)
2. Программное обеспечение. Прикладное программное обеспечение. Текстовые редакторы.
3. Информационные технологии в промышленности, компьютерные технологии. Интернет-технологии, как часть информационных технологий.

Литература:

1. Советов, Б. Я. Информационные технологии: Учеб. для студентов вузов - М.: Высш. шк., 2003. - 263 с.
2. Бородакий, Ю. В. Информационные технологии: Методы, процессы, системы - М.: Радио и связь, 2004. – 451 с.
3. Попов В. Б. Основы информационных технологий, Учебное пособие. - М.: Финансы и статистика, 2002.

Архитектура компьютерных систем

1. Основные функциональные элементы ЭВМ (регистр хранения, регистр сдвига). Классификация запоминающих устройств.
2. Регистровая структура процессора i8086 (регистры общего назначения, сегментные регистры, регистр флагов, регистр IP (InstructionPointer)).
3. Режимы адресации процессора i8086 и способы их задания. Машинное представление команд различных форматов, использующих различные режимы адресации операндов (ассемблирование). Восстановление символической записи команды по ее машинному коду (дизассемблирование).
4. Адресация памяти в реальном режиме. Сегменты и смещения. Адресация памяти в защищенном режиме. Селекторы и дескрипторы. Уровни привилегий. Прерывания.

Литература:

1. Брэй Барри. Микропроцессоры Intel. Издательство: БХВ-Петербург Год издания: 2005 1328 с
2. П.С.Довгий, В.И.Поляков. Прикладная архитектура процессора Intel 8086. - Санкт-Петербург, 2006г. – 32 с.
3. В.В. Гуров, В. О. Чуканов. Архитектура и организация ЭВМ. – М. «Издательство ИНТУИТ», 2005 г., -124 с.

Объектно-ориентированное программирование

1. Базовые типы данных, константы базовых типов. Понятие оператора.
2. Понятие цикла, конструкция while, конструкция do while. Цикл for. Массивы. Генератор случайных чисел.

3. Понятие инкапсуляции, класса и объекта. Спецификаторы доступа public, private, protected.
4. Особенности объявления и использования данных – членов класса. Применение конструкторов для инициализации данных класса.
5. Основные термины библиотеки STL. Группы алгоритмов в STL.

Литература:

1. Страstrup Б. Язык программирования C++. 3-е изд./Пер. с англ.-СПб.; М.: «Невский Диалект» - «Издательство БИНОМ», 1999 г.-991 с.
2. Шаммас Н.К. Основы C++ и объектно-ориентированного программирования. – К.: Диалектика, 1996. –448с., ил.
3. Аммерааль Л. STL для программистов на C++. Пер. с англ. – ДМК, 1999 -240 с.
4. Дейтел Х. М, Дейтел П. Дж. Как программировать на C++. Пер. с англ. – М.: ЗАО «Издательство БИНОМ», 2000 г. – 1024 с.

Теория информации и кодирования

1. Количественная оценка информации. Энтропия (безусловная и условная). Энтропия объединения.
2. Коды. Представление кодов. Понятие о кодировании. Избыточность информации.
3. Основные теоремы кодирования канала связи без шума.
4. Оптимальное кодирование. Метод Шеннона-Фано. Метод Хаффмена.

Литература:

1. Цымбал В.П. Теория информации и кодирование. -К.:Вища шк.,1992.
2. Бэрлекэмп Э. Алгебраическая теория кодирования. –М.Мир,1971.
3. Цымбал В.П. Задачник по теории информации и кодирования.- К.:Вища шк.,1976.
4. Панин В.В. Основы теории информации.-М.:Бином,2007.

Комплексные системы защиты информации: проектирование, внедрение, сопровождение

1. Организация защиты информации от несанкционированного доступа. Разграничение доступа к информации
2. Классификация информации по типам и видам. Структура защищаемых документопотоков.
3. Классификация информации по уровням требований к ее защищенности
4. Операции над нечеткими множествами. Порядок получения результата прогноза на основе теории нечетких множеств.
5. Основные принципы работы искусственных нейронных сетей.
6. Определение функции риска, выживаемости и плотности распределения вероятностей в обработке факторов, влияющих на эффективность защиты информационной системы.

Литература:

1. Гитман М. Б. Введение в теорию нечетких множеств и интервальную математику: Ч. 1: Применение лингвистической переменной в процессе принятия решений. // Учебное пособие. – Пермь: Изд-во Перм. гос. техн. ун-та, 1998. – 45 с.
2. Зайченко Ю. П. Нечеткие модели и методы в интеллектуальных системах. Учеб.пособ. для студ. высш. уч. зав. / Ю.П.Зайченко. – К.: Слово, 2008. – 344с.
3. Каллан Р. Основные концепции нейронных сетей / Роберт Каллан. Пер. с англ. – М.: Издательский дом «Вильямс», 2001. – 288с.
4. Круглов В.В. Нечеткая логика и искусственные нейронные сети: Учеб.пособие / В. В.Круглов, М.И.Дли, Р.Ю.Голунов. – М.: Изд-во физ.-мат. лит., 2005. – 225с.
5. Нейронные сети. STATISTICA NeuralNetwork: Методология и технология современного анализа данных / Под.ред. В.П.Боровикова. – 2-е изд., перераб. и доп. – М.: Горячая линия – Телеком, 2008. – 492с.

Прикладная криптология

1. Основные модели шифров и их свойства; простейшие шифры и их свойства; композиции шифров; криптографическая стойкость шифров
2. Симметричные и асимметричные системы шифрования, основные преимущества и недостатки.
3. Принципы организации сетей конфиденциальной связи; понятие о криптографических протоколах, протоколах распределения ключей и установление подлинности; парольные системы разграничения доступа; электронная цифровая подпись.
4. Криптоатаки: атака методом исчерпывающего перебора, имитация и подмена сообщения (коллизии хеш-функций), подмена открытых ключей.
5. Принципы защиты информации в компьютерных системах и сетях с помощью стеганографических методов. Сферы применения стеганографии; требования к построению стеганографических систем; протоколы стеганографических систем.

Литература:

1. Сمارт Н. Криптография. М.: Техносфера, 2005. – 528 с.
2. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. СПб.: Изд-во «Лань», 2001. – 224 с.
3. Яценко В.В. Введение в криптографию. СПб.: Питер, 2001. – 288 с.
4. Бассар Ж. Современная криптологи. М.: Изд-ско-полиграф. фирма ПОЛИМЕД, 1999. – 176 с.

Информационно коммуникационные системы

1. Телеграфные уравнения. Первичные и вторичные параметры длинной линии. Режимы работы длинной линии без потерь. Отрезок линии конечной длины как элемент цепи. Способы согласования.

2. Математические основы диаграммы Вольперта-Смита. Определение коэффициента бегущей волны (стоячей волны) в линии с известной нагрузкой. Определение входного сопротивления линии.
3. Характеристики и параметры антенны в режиме передачи и приема. Типы антенных решеток и их характеристики. Теорема перемножения диаграмм направленности.
4. Эталонная модель взаимодействия открытых систем (OSI). Инкапсуляция данных. Физический уровень. Канальный уровень. Типы сетевых устройств и их функции
5. Стекпротоколов TCP/IP. Типы адресов стека TCP/IP. IP-адресация (структура IP-адреса, классы IP-адресов, протоколы IPv4 и IPv6). Система доменных имен (протокол DNS). Протоколы транспортного уровня (протоколы TCP, UDP)

Литература:

1. Ефимов И.Е., Останькович Г.А. Радиочастотные линии передачи. М.: Связь, 1977. - 207 с.
2. Сазонов Д.М. Антенны и устройства СВЧ. – М.: Издательство: Высшая школа, 1988 г. - 427 с.
3. Пудовкин А.П. Основы теории антенн: учебное пособие /А.П. Пудовкин, Ю.Н. Панасюк, А.А. Иванков. -Тамбов: Изд-во ГОУ ВПО ТГТУ, 2011. – 92 с.
4. Олифер В.Г. Олифер Н.А. Компьютерные сети. Принципы технологии протоколы. СПб.: - Питер, 2010, 916 с. 4 изд.
5. Вито Амато. Основы организации сетей Cisco, том 1, испр. изд. : Пер. с англ. - М. : Издательский дом "Вильямс", 2004. — 512 с.
6. Вито Амато. Основы организации сетей Cisco. Том 2 Издательство: М.: Вильямс Год выпуска: 2004, 2-е изд. Число страниц: 466.

Защита информации в информационно-коммуникационных системах

1. Физические поля, создающие каналы утечки информации. Многообразие физических полей.
2. Угрозы безопасности информации и информационные атаки. Информационные угрозы.
3. Защита информации в каналах связи и передачи данных. Стандарты симметричных криптосистем.

Литература:

1. Куприянов А.И., Сахаров А.В., Шевцов В.А. Основы защиты информации.
2. Хорев А.А. Способы и средства защиты информации. Москва. 2000.
3. Шеннон К.Э. Теория связи в секретных системах. Работы по теории информации и кибернетике. Москва. Иностранная литература. 1963.

Системы технической защиты информации

1. Средства перехвата аудиоинформации. Акустические антенны.
2. Средства обеспечения скрытности оперативной звукозаписи
3. Перехват информации в GSM.
4. Методы и средства выявления закладных устройств.

Литература:

1. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами. Учебное пособие. СПб, НИУ ИТМО, 2012.
2. Безбогов А.А., Яковлев А.В., Шамкин В.Н. Методы и средства защиты компьютерной информации. Тамбов, издательство ТГТУ. 2006.
3. Исаев А.Б. Современные технические методы и средства защиты информации. Москва, РУДН, 2008.

Цифровая обработка сигналов

1. Сложение двух сигналов
2. Дельта функция и белый шум.
3. Представление системы в частотной области

Литература:

1. Сато Ю. Без паники! Цифровая обработка сигналов. Москва. ДОДЭКА. 2010.
2. Основы цифровой обработки сигналов . Курс лекций. // Солонина, Улахович, Арбузов, Соловьева, Гук. СПб: С.-Петербург. 2003.
3. Лукин А. Введение в цифровую обработку сигналов. МГУ. 2002

Системы цифровой обработки сигналов

1. Структура типовой системы на базе ЦПОС
2. Структура цифровой вычислительной машины
3. Пример архитектуры TMS320C5X

Литература:

1. Курс лекций по системам цифровой обработки сигналов
2. Гольденберг Л.М., Матюшкин Б.Д., Поляк М.Н. Цифровая обработка сигналов. М., Радио и связь. 1990.
3. Цифровые процессоры обработки сигналов. Справочник. Под ред. Остапенко А.Г., - М.: Радио и связь, 1994.
4. Вишняков В.А. Системы цифровой обработки сигналов. Рыбинск. РГАТА, 2000.

4. Структура билета

Билет состоит из двух частей.

Первая (тестовая) часть содержит 20 тестовых заданий. На каждый вопрос из первой части предлагается три или четыре варианта ответа, обозначенных буквами, причём верным является только один из вариантов ответа. Среди вариантов ответов необходимо найти наиболее правильное и полное теоретическое положение, фрагмент формулировки, тезис, отвечающий требованиям, заданным в условии.

Вторая (творческая) часть задания содержит два вопроса, требующие развёрнутых ответов, пояснений, исследования ситуации, выполнения расчётов или применения других практических навыков. Цель этой части задания – выявление глубины теоретических и практических знаний абитуриента, понимания им сути изученного материала, умения применять знания в практических расчётах, анализировать и исследовать результаты расчётов.

Ниже приведена структура билета.

ПАКЕТ 1

УТВЕРЖДЕНО:

на заседании Ученого совета
физико-технического факультета
протокол № 6 от 15.02.2019

ГОУ ВПО «Донецкий национальный университет»

Физико-технический факультет

Профильный экзамен по

ОП

Форма обучения

Направление подготовки:

СПЕЦИАЛЬНОСТИ

Магистратура

Очная, заочная

10.04.01 Информационная безопасность

Вариант 1

Тестовые задания (60 баллов)

Приведены 20 вопросов с вариантами ответов (правильный ответ необходимо отметить знаком «✓»)

Творческие задания (40 баллов)

1. Творческое задание.

2. Творческое задание.

Председатель приёмной комиссии

С.В. Беспалова

Председатель экзаменационной комиссии

С.А. Фоменко

5. Образец бланка ответов

ГОУ ВПО «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ»

ШИФР

Физико-технический факультет

Профильный экзамен по Специальности

Оценка

Лист ответов

Билет № _____

Тестовые задания

№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	Итого:
А																					
Б																					
В																					
Г																					
+																					

Творческие задания

6. Критерии оценивания письменных ответов на вступительном испытании

Каждый правильный ответ на вопрос из первой (тестовой) части оценивается в 3 балла. Каждый ответ на вопросы из второй (творческой) части оценивается от 0 до 20 баллов по следующим критериям:

Баллы	Критерии оценивания
0-5	Ответ, в котором допущены грубые ошибки при изложении теоретического материала или в практических расчётах. При отсутствии ответа выставляется 0 баллов.
6-10	Неполный ответ, ответ без чёткого указания причин и следствий, с ошибками в изложении материала или практических расчетах.
11-15	Полный, но недостаточно логичный или обоснованный ответ на вопрос, с несущественными ошибками в изложении материала и практических расчетах.
16-20	Полный, чёткий, логичный и обоснованный ответ на вопрос оценивается в 20 баллов. Оценка может быть снижена за неточности в формулировках и вычислениях.

Критерии утверждены ученым советом физико-технического факультета, протокол № 6 от 15.02.2019 года.

Таким образом, максимальное количество баллов за выполнение первой части задания составляет **60** баллов, за выполнение второй части задания – **40** баллов. Следовательно, максимальное количество баллов, полученных на вступительном испытании, составляет **100** баллов.

Соответственно, по ниже приведенной схеме осуществляется перевод баллов в пятибалльную систему:

100-балльная шкала	5-балльная шкала
0-59	«2» (неудовлетворительно)
60-74	«3» (удовлетворительно)
75-89	«4» (хорошо)
90-100	«5» (отлично)