МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования «Приазовский государственный технический университет»

УТВЕРЖДАЮ
И.о. ректора ФГБОУ ВО «ПГТУ»
_____ И.В. Кущенко
МП
«12» 04 2025

ПРОГРАММА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ по ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
для поступающих на обучение по образовательным программам высшего образования – программе магистратуры

Мариуполь, 2025

1. Пояснительная записка

Цели и задачи вступительного испытания

Программа вступительного испытания по информационной безопасности разработана на основании Федеральных государственных образовательных стандартов высшего образования.

Целью вступительного испытания является определение уровня подготовки поступающих и оценки их способности для дальнейшего обучения по программам магистратуры

Требования к уровню подготовки поступающих

Программа испытания сформирована непосредственно на основе требований к предметным результатам освоения основной образовательной программы по информационной безопасности федерального государственного образовательного стандарта высшего образования.

На вступительном испытании соискатель должен продемонстрировать основные компетенции, сформированные в результате освоения дисциплин «Методы программирования», «Операционные системы», «Компьютерные сети», «Основы информационной безопасности», «Модели безопасности компьютерных систем», «Криптографические методы защиты информации», «Программно-аппаратные средства обеспечения информационной безопасности».

Контрольно-измерительные материалы

Контрольно-измерительные материалы вступительного испытания по информационной безопасности представляют собой следующие виды заданий:

− задания на выбор единственного ответа из предложенного списка ответов;

− задания на выбор одного или нескольких правильных ответов из предложенного списка ответов (задания множественного выбора).

Форма проведения вступительного испытания

Вступительное испытание проводится в форме тестирования.

Продолжительность вступительного испытания

На выполнение экзаменационных заданий отводится 2 часа (120 минут).

Шкала оценивания

Результат вступительного испытания оценивается по 100-балльной шкале. Минимальное количество баллов, подтверждающее успешное прохождение вступительного испытания, устанавливается Правилами приема.

Критерии оценивания

Оценивание вступительного испытания по информационной безопасности в форме тестирования осуществляется посредством проверки (ручной и/или компьютерной) ответов на тестовые задания. Задания оцениваются разным количеством баллов в зависимости от их

типа и степени сложности. Баллы, полученные экзаменуемым за правильно выполненные задания, суммируются.

Вопросы теста включают задания, распределенные по категориям сложности:

–вопрос с единственно верным ответом из предложенного списка ответов (за правильно выполненное задание этой категории абитуриент получает первичный балл, установленный для заданий этой категории; отсутствие ответа или неправильный ответ оценивается 0 баллов);

–вопрос с множественным выбором (считается каждый верный ответ, таким образом, за 6 вопросов на соответствие, абитуриент может получить от 1 до 6; во всех других случаях выставляется 0 баллов).

Язык проведения вступительного испытания

Вступительное испытание проводится на русском языке.

2. Содержание программы

Темы вступительных испытаний по информатике и вычислительной технике

На основе указанных выше требований определены темы испытания:

Раздел 1. Методы программирования.

– Основные алгоритмы поиска и сортировки. Сортировка массивов и файлов, поиск в глубину и в ширину.
– Рекурсивные алгоритмы. Виды и характеристики рекурсии.
– Рекурсивные структуры данных и их применение.
– Деревья как структуры данных. Основные виды деревьев, их сравнительные характеристики.
– Поиск с помощью хэширования. Хэш-функции в программировании.
– Методы оптимизации программ. Машинно-зависимая и машиннонезависимая оптимизация.
– Методы тестирования и отладки. Тестирование черного и белого ящика.
– Переносимость программ. Правила написания переносимых программ.
– Параллельное программирование. Особенности программирования параллельных программ на GPU.

Раздел 2. Операционные системы.

– Функции операционных систем, архитектуры операционных систем.
– Планирование процессов и потоков.
– Взаимодействие процессов, взаимоисключения и синхронизация процессов.
– Управление памятью. Виртуальная память.
– Организация ввода/вывода.
– Файловые системы.
– Механизмы защиты операционных систем.
– Системы реального времени.
– Многопроцессорные системы.
– Механизмы виртуализации операционных систем.
– Операционная система UNIX. Архитектура, механизмы управления процессами и памятью.
– Операционная система UNIX. Организация файловой системы.
– Операционная система Windows. Архитектура, механизмы управления процессами и памятью.

– Операционная система Windows. Файловые системы, сервисы, системный реестр.
– Операционные системы Windows и UNIX. Подсистемы безопасности.
– Служба каталога.

Раздел 3. Компьютерные сети.

– Модель OSI ISO. Модель TCP\IP. Уровни моделей. Инкапсуляция данных.
– Витая пара, виды. Коаксиальный кабель. Волоконная оптика.
– Протоколы множественного доступа с контролем несущей. Кадр, структура. Адресация.
– Ethernet. Уровень MAC. Типы адресов.
– Протокол ARP. Взаимосвязь IP и MAC-адресов.
– Протокол IP. Инкапсуляция данных. Заголовок.
– Разделение сети на подсети. Схемы адресации. VLSM.
– Транспортный уровень. Структура данных. Адресация.
– Уровень приложений. Протоколы. Служба DNS.
– VLAN. Назначение, типы. Транковые порты. Протокол DTP.
– Статическая маршрутизация. Типы маршрутов.
– Динамическая маршрутизация. Протоколы состояния канала. Алгоритм Дейкстра. Маршрутные обновления.
– Протокол DHCP. Поддержка IPv6. Технология SLAAC.
– NAT. Назначение, преимущества, типы.

Раздел 4. Основы информационной безопасности.

– Группы причин нарушения безопасности компьютерных систем.
– Состояние правового обеспечения информационной безопасности, система стандартов в области информационной безопасности.
– Лицензирование деятельности в области информационной безопасности.
– Системы сертификации в области информационной безопасности.
– Понятие угроз информационной безопасности, их систематизация.
– Разрушающие программные средства.
– Модель нарушителя.
– Сценарий компьютерной атаки.
– Функции защиты.
– Виды и средства контроля безопасности.
– Системы и средства обнаружения компьютерных атак.
– Технология построения защищенных информационных систем.

Раздел 5. Модели безопасности компьютерных систем.

– Дискреционный контроль доступа. Модель Харрисона–Руззо– Ульмана: основные определения. Теорема безопасности.
– Модель Харрисона–Руззо–Ульмана. Теорема о разрешимости проблемы безопасности в частных и в общем случае. Монитор безопасности пересылок.
– Модель типизированной матрицы доступа (ТМД), монотонная ТМД.
– Мандатный контроль доступа. Модель Белла и ЛаПадулы: основные определения.
– Модель Белла и ЛаПадулы: формальное описание. Основная теорема безопасности. Критика модели Белла и ЛаПадулы.
– Модели целостности. Модель Биба: описание, теорема о пути передачи информации. Критика модели Биба.
– Модель безопасных функций перехода. Теорема Мак-Лина.
– Модель уполномоченных субъектов.
– Модель совместного доступа. Критерий безопасности. Безопасная функция перехода для моделей совместного доступа.
– Ролевой контроль доступа. Критерии безопасности. Достоинства и недостатки.
– Модель Take-Grant. Основные определения. Разделение права доступа в терминах модели Take-Grant, необходимые и достаточные условия разделения права.

– Модель Кларка-Вилсона: область применения, цели, описание.
– Модель Китайской стены: область применения, цели, описание.

Раздел 6. Криптографические методы защиты информации.

– Основные понятия симметричной криптографии. Понятие стойкости криптографического алгоритма. Простейшие шифры и их свойства.
– Криптографические функции хэширования.
– Основные понятия криптографии с открытым ключом. Вычислимая в одну сторону функция. Функция с лазейкой. Шифрование с открытым ключом. Цифровая подпись.
– Протоколы на основе задачи разложения числа на множители. RSA. Методы решения задачи разложения числа на множители.
– Протоколы на основе задачи дискретного логарифмирования. Схема Эль-Гамаля. Методы решения задачи дискретного логарифмирования.

Раздел 7. Программно-аппаратные средства обеспечения информационной безопасности.

– Основы сетевого и межсетевого взаимодействия.
– Сущность и основные виды вредоносного программного обеспечения.
– Основные методы защиты от вредоносного ПО.
– Виды удаленных сетевых атак.
– Основные механизмы обеспечения информационной безопасности.
– Основные технологии межсетевого экранирования.
– Системы обнаружения сетевых атак и вторжений.
– Методы обнаружения сетевых аномалий.
– Виртуальные частные сети. Удостоверяющие центры и сертификаты.
– Технология IPSec.

Раздел 7. Программно-аппаратные средства обеспечения информационной безопасности.

– Основы сетевого и межсетевого взаимодействия.
– Сущность и основные виды вредоносного программного обеспечения.
– Основные методы защиты от вредоносного ПО.
– Виды удаленных сетевых атак.
– Основные механизмы обеспечения информационной безопасности.
– Основные технологии межсетевого экранирования.
– Системы обнаружения сетевых атак и вторжений.
– Методы обнаружения сетевых аномалий.
– Виртуальные частные сети. Удостоверяющие центры и сертификаты.
– Технология IPSec.

Фонд оценочных средств

Содержание тестовых заданий по информационной безопасности соответствует основным темам, включенным в программу вступительного испытания.

3. Литература и материалы для подготовки

Основная литература:

1. Таненбаум, Э. Современные операционные системы / Э. Таненбаум ; Х. Бос. – 4-е изд . – М. [и др.] : Питер, 2017 . – 1120 с.
2. Столлингс, В. Операционные системы : Внутреннее устройство и принципы проектирования: Пер. с англ. / В. Столлингс . – 4-е изд . – М. : Вильямс, 2002 . – 843 с.
3. Робачевский, А.М. Операционная система UNIX : Учеб. пособие для вузов / А.М. Робачевский . – СПб. : БХВ-Петербург, 2007 . – 656 с.
4. Соломон, Д. Внутреннее устройство Microsoft Windows Основные подсистемы ОС : / М. Руссинович, Д. Соломон, А. Ионеску. – СПб : Питер, 2014 . – 672 с.

5. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер – СПб. Питер, 2016.
6. Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл – СПб. Питер, 2016.
7. Мэрфи, Н. IPv6. Администрирование сетей / Н. Мэрфи, Д. Мэлоун – СПб. КУДИЦ-Пресс, 2007.
8. Нестеров, С.А. Основы информационной безопасности. / С.А. Нестеров. – СПб. : Лань, 2016.— 324 с.
9. Партыка Т.В. Информационная безопасность / Т.В. Партыка. – 5-е изд . – М. : Форум, 2014 . – 432 с.
10. Родичев, Ю.А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие / Ю.А. Родичев. – СПб : Питер, 2017. – 256 с.

Дополнительная литература:

1. Гайдамакин, Н.А. Теоретические основы компьютерной безопасности / Н.А. Гайдамакин //Екатеринбург: Изд-во Урал. ун-та, 2008. – http://elar.urfu.ru/bitstream/10995/1778/5/1335332_schoolbook.pdf.
2. Зегжда, П.Д. Теоретические основы компьютерной безопасности: Курс лекций / Зегжда П.Д., Зегжда Д.П. – СПб., 2008.
3. Девянин, П.Д. Модели безопасности компьютерных систем: Учеб.
пособие для студ. высш. учеб. заведений / П.Д. Девянин. – М.: Издательский центр «Академия», 2005 – 144с.
4.Введение в криптографию / Под общ. ред. В. В. Ященко. - 4-е изд., доп. М.: МЦНМО, 2012. http://cryptography.ru/wpcontent/uploads/2013/09/intro_to_crypto.pdf.
5. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. 3-е изд., испр. и доп. — М.: Гелиос АРВ, 2005. — 480 с.
6.Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов // http://www.bnti.ru/dbtexts/ipks/old/analmat/1_2002/crypto.pdf.
7.Ишмухаметов, Ш.Т. Методы факторизации натуральных чисел / Ш.Т. Ишмухаметов // http://old.kpfu.ru/f9/bibl/Monograph_ishm.pdf.
8.Программно-аппаратные средства защиты информации / В.В. Платонов — М.: Издательский центр «Академия», 2013. — 336 с. — http://itebooks.ru/publ/it_secutity/programmno_apparatnye_sredstva_zashhity_informacii/ 15-1-0-745.
9.Информационная безопасность компьютерных систем и сетей:
Учебное пособие / В.Ф. Шаньгин — М.: ИД ФОРУМ: ИНФРА-М, 2012. — 416 с. — http://znanium.com/bookread.php?book=335362.
10.Башлы, П.Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — М.:РИОР, 2013. — 222 с. — http://znanium.com/bookread.php?book=405000.