

  
«УТВЕРЖДАЮ»  
Ректор ГУАП  
Ю.А. Антохина  
« 19 » 01 2024



**ПРОГРАММА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ ПРИ ПРИЕМЕ НА  
ОБУЧЕНИЕ ПО ПРОГРАММЕ ПОДГОТОВКИ НАУЧНЫХ И НАУЧНО-  
ПЕДАГОГИЧЕСКИХ КАДРОВ В АСПИРАНТУРЕ ПО НАУЧНОЙ  
СПЕЦИАЛЬНОСТИ**

**2.3.6. «Методы и системы защиты информации, информационная  
безопасность»**

# **1. ОБЩИЕ ПОЛОЖЕНИЯ ПО ПРОВЕДЕНИЮ ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ ПО ПРИЕМУ В АСПИРАНТУРУ ПО НАУЧНОЙ СПЕЦИАЛЬНОСТИ 2.3.6. «МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

1.1. Настоящая Программа, составленная в соответствии с федеральными государственными образовательными стандартами ВО по направлению подготовки 10.04.01 «Информационная безопасность», устанавливает содержание вступительных испытаний с целью определения подготовленности поступающего и наличия способностей для обучения в аспирантуре по научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность».

1.2. Конечной целью вступительного испытания является определение уровня знаний и компетенций поступающего по 100-балльной шкале.

## **2. ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПРОВЕДЕНИЯ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ**

1. Информация, сообщение, информационные системы и процессы как объекты информационной безопасности. Основные свойства информации. Мера количества информации. Энтропия. Модели стоимости информации.

2. Случайные события. Полная группа событий. Зависимые и независимые случайные события. Вероятность случайного события.

3. Условная вероятность. Формула полной вероятности. Теорема Байеса.

4. Случайные величины и их характеристики: функция распределения, моменты, характеристические функции.

5. Дискретные и непрерывные случайные величины. Биномиальный закон распределения. Нормальный закон распределения. Центральная предельная теорема Ляпунова.

6. Основные задачи математической статистики: точечная оценка, построение доверительного интервала, различение статистических гипотез.

7. Основы теории чисел. Понятие группы, кольца, поля.

8. Криптографические методы защиты информации. Основные постулаты криптографии. Исторические шифры.

9. Криптоаналитика. Теоретическая, практическая и временная стойкость системы криптографической защиты. Современные поточные и блочные алгоритмы шифрования.

10. Системы симметричного шифрования. Вопросы генерации и распределения ключей. Обоснование надежности криптографической защиты.

11. Системы асимметричного шифрования, открытый ключ, электронная подпись. Атака «человек посередине».

12. Псевдослучайные последовательности: области применения в задачах обеспечения информационной безопасности; методы получения; способы оценки качества.

13. Современная криптография с открытым ключом: основные идеи, концепция. Криптосистемы RSA, El Gamal, рюкзака.

14. Электронная цифровая подпись: основные идеи, концепции, Подпись RSA, El Gamal. Отрицаемая и неотрицаемая подпись.

15. Криптографические протоколы. Протоколы аутентификации без разглашением, протокол подбрасывания монетки.

16. Математический аппарат для криптографии: китайская теорема об остатках, расширенный алгоритм Евклида, арифметика в конечных полях.

17. Эллиптические кривые в криптографии. Основные концепции и идеи. Криптосистема ElGamal, протокол Мессе-Омура.
18. Пороговые схемы разделения секрета на Китайской теореме об остатках, интерполяционной формуле Лагранжа.
19. Протоколы аутентификации без разглашения.
20. Использование хэш-функций. Одноразовые подписи на цепочках Лампорта и на дереве Меркле.
21. Слепая подпись Чаума и ее использование в протоколах электронного голосования.
22. Стеганография. Основные свойства, подходы к реализации, использование алгоритмов LSB и психовизуальных/психоакустических эффектов.
23. Атаки на стеганографические методы. Понятие цифрового водяного знака.
24. Поточковые шифры. Использование регистров сдвига с линейной обратной связью и их суперпозиций. Понятие линейной сложности и профиля линейной сложности. Расчет линейной сложности.
25. Стандарт шифрования в GSM A5. Принцип построения основные свойства, известные атаки.
26. Методы и протоколы защиты информации от несанкционированного использования и копирования.
27. Классификация вредоносных программ. Классические определения четырех основных типов вредоносных программ. Методы борьбы с вредоносными программами.
28. Постквантовая криптография как отдельный раздел криптографии. Основные концепции и идеи.
29. Технология блокчейн. Принцип работы. Публичный и приватный блокчейн.
30. Проблемы безопасности сетевых технологий. Сетевая модель OSI/ISO. Уровни модели OSI.
31. Риск информационной безопасности: понятие; задача управления рисками; методологические основы и инструментальные средства оценки рисков информационной безопасности.