# ***Программа вступительного экзамена по направлению подготовки 10.06.01«Информационная безопасность»***

**Целью** вступительного испытания является оценка уровня освоения поступающим компетенций, необходимых для обучения по направлению ***«Информационная безопасность»***по образовательным программам высшего образования - программам подготовки научно-педагогических кадров в аспирантуре.

**Программы вступительных испытаний при приеме на обучение в аспирантуре формируются** на основе федеральных государственных образовательных стандартов высшего образования (СУОС Университета ИТМО) по программам специалитета или магистратуры.

**Форма вступительного испытания:** устно-письменная

**Форма вступительного испытания с использованием дистанционных технологий:** тест, устно-письменная

**Продолжительность** проведения вступительного испытания. Продолжительность вступительного испытания - не более 90 минут.

**Критерии оценивания:** “неудовлетворительно”, “Удовлетворительно”, “Хорошо”, “Отлично”

**Минимальный проходной балл,** подтверждающий успешное прохождение вступительных испытаний: оценка “удовлетворительно”.

**Перечень принадлежностей**, которые поступающий имеет право пронести в аудиторию во время проведения вступительного испытания: письменные принадлежности, непрограммируемый калькулятор.

# **Профиль подготовки 05.13.19 «Методы и системы защиты информации. Информационная безопасность»**

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. Биноминальный закон распределения. Нормальный закон распределения. Центральная предельная теорема Ляпунова.
6. Основные задачи математической статистики: точечная оценка, построение доверительного интервала, различение статистических гипотез.
7. Понятие угрозы информационной безопасности. Виды угроз. Модель угроз. Методы оценки уязвимостей автоматизированных систем.
8. Понятие модели нарушителя. Цель, задачи, способы формирования и представления модели нарушителя.
9. Построение систем защиты от угрозы нарушения конфиденциальности информации. Построение систем защиты от угрозы нарушения целостности информации. Построение систем защиты от угрозы отказа доступа к информации.
10. Модели безопасности. Модель матрицы доступов HRU. Модель распространения прав доступа Take-Grant. Модель системы безопасности Белла-Лападула.
11. Цели и концептуальные основы защиты информации. Современная концепция информационной безопасности. Место информационной безопасности в системе национальной безопасности.
12. Критерии, условия и принципы отнесения информации к защищаемой. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности.
13. Виды уязвимостей информации и формы ее проявления. Каналы и методы несанкционированного доступа к конфиденциальной информации.
14. Методологические основы защиты информации и принципы ее организации. Комплексные системы защиты информации.
15. Составные части информационной безопасности. Виды обеспечения информационной безопасности. Классификация методов и средств защиты информации.
16. Нормативно-правовые акты Российской Федерации в области информационной безопасности.
17. Математические модели: виды, возможности, ограничения, области применения. Современные инструментальные средства математического моделирования.
18. Имитационное моделирование: понятие, цели, области применения, возможности, ограничения. Современные инструментальные средства имитационного моделирования.
19. Состав и содержание основных этапов модельного эксперимента.
20. Статические и динамические модели. Моделирование динамических процессов реакциями элементарных динамических звеньев.
21. Обработка данных наблюдений. Сущность и подходы.
22. Задачи регрессии как один из путей построения моделей. Определение параметров регрессии. Алгоритм МНК.
23. Криптографические методы зашиты информации. Основные постулаты криптографии. Исторические шифры.
24. Криптоаналитика. Теоретическая, практическая и временная стойкость системы криптографической защиты. Современные поточные и блочные алгоритмы шифрования.
25. Системы симметричного шифрования. Вопросы генерации и распределения ключей. Обоснование надежности криптографической защиты.
26. Системы асимметричного шифрования, открытый ключ, электронная подпись. Атака «человек посредине».
27. Псевдослучайные последовательности: области применения в задачах обеспечения информационной безопасности; методы получения; способы оценки качества.
28. Проблемы безопасности сетевых технологий. Сетевая модель OSI/ISO. Уровни модели OSI.
29. Риск информационной безопасности: понятие; задача управления рисками; методологические основы и инструментальные средства оценки рисков информационной безопасности.
30. Обзор информационных ресурсов в области информационной безопасности: авторы, фундаментальные монографии и статьи, нормативно-правовые документы, ресурсы научных школ, профессиональные сообщества.