

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф – Программа вступительных испытаний		

УТВЕРЖДАЮ:

Председатель приемной комиссии УлГУ

Б.М. Костишко

Б.М. Костишко 2022 г.



ПРОГРАММА

вступительных испытаний по научной специальности

2.3.6. МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

для поступающих на обучение по программам подготовки
научных и научно-педагогических кадров в аспирантуре
Ульяновского государственного университета

Сведения о разработчиках:

ФИО	Аббревиатура кафедры	Ученая степень, звание
Смагин Алексей Аркадьевич	ТТС	д.тех.н., профессор

Ульяновск, 2022

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф – Программа вступительных испытаний		

1. Общие положения

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 УлГУ.

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.

1.1. Организация и проведение вступительного испытания осуществляется в соответствии с Правилами приема, утвержденными решением Ученого совета УлГУ, действующими на текущий год поступления.

1.2. 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 форме устного экзамена в соответствии с перечнем тем и (или) вопросов, установленных данной Программой.

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): очно и дистанционно.

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.

Примерный перечень тем и вопросов для подготовки к сдаче экзамена и формирования билетов.

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф – Программа вступительных испытаний		

2.3.6. МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Раздел 1. Избранные разделы математики и информатики.

1. Информация, сообщения, информационные системы и процессы как объекты информационной безопасности.
2. Основные свойства информации. Мера количества информации. Энтропия.
3. Случайные события. Полная группа событий. Зависимые и независимые случайные события. Вероятность случайного события.
4. Условная вероятность. Формула полной вероятности. Теорема Байеса.
5. Случайные величины и их характеристики: функция распределения, моменты, характеристические функции.
6. Дискретные и непрерывные случайные величины. Биноминальный закон распределения. Нормальный закон распределения. Центральная предельная теорема Ляпунова.
7. Основные задачи математической статистики: точечная оценка, построение доверительного интервала, различение статистических гипотез.
8. Сетевая модель OSI/ISO. Уровни модели OSI.
9. Сетевая модель OSI/ISO. Примеры протоколов.

Раздел 2. Теоретические основы информационной безопасности

1. Понятие угрозы информационной безопасности. Виды угроз.
2. Основные методы реализации угроз информационной безопасности. Основные принципы обеспечения информационной безопасности в АС.
3. Методы оценки угроз ИБ. Модель угроз.
4. Причины, виды и каналы утечки информации.
5. Построение систем защиты от угрозы нарушения конфиденциальности информации.
6. Построение систем защиты от угрозы нарушения целостности информации.
7. Построение систем защиты от угрозы отказа доступа к информации.
8. Политика безопасности. Понятие политики безопасности. Понятия доступа и монитора безопасности. Основные типы политики безопасности.
9. Модели безопасности. Модель матрицы доступов HRU.
10. Модель распространения прав доступа Take-Grant.
11. Модель системы безопасности Белла-Лападула.
12. Основные критерии защищенности АС. Классификация систем защиты АС. Руководящие документы Государственной технической комиссии России.
13. Общие критерии (ОК). Основные положения ОК.

Раздел 3. Основы криптографической защиты информации.

1. Криптографические методы защиты информации. Основные понятия криптографии. Исторические шифры.
2. Теоретическая, практическая и временная стойкость системы криптографической защиты.
3. Методы получения псевдослучайных последовательностей. Современные поточные и блочные алгоритмы шифрования.
4. Системы симметричного шифрования.

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф – Программа вступительных испытаний		

5. Системы асимметричного шифрования, открытый ключ, электронная подпись.
6. Вопросы генерации и распределения ключей. Обоснование надежности криптографической защиты.

Перечень вопросов

1. Информация, сообщения, информационные системы и процессы как объекты информационной безопасности.
2. Основные свойства информации. Мера количества информации. Энтропия.
3. Случайные события. Полная группа событий. Зависимые и независимые случайные события. Вероятность случайного события.
4. Условная вероятность. Формула полной вероятности. Теорема Байеса.
5. Случайные величины и их характеристики: функция распределения, моменты, характеристические функции.
6. Дискретные и непрерывные случайные величины. Биноминальный закон распределения. Нормальный закон распределения. Центральная предельная теорема Ляпунова.
7. Основные задачи математической статистики: точечная оценка, построение доверительного интервала, различение статистических гипотез.
8. Сетевая модель OSI/ISO. Уровни модели OSI.
9. Сетевая модель OSI/ISO. Примеры протоколов.
10. Понятие угрозы информационной безопасности. Виды угроз.
11. Основные методы реализации угроз информационной безопасности. Основные принципы обеспечения информационной безопасности в АС.
12. Методы оценки угроз ИБ. Модель угроз.
13. Причины, виды и каналы утечки информации.
14. Построение систем защиты от угрозы нарушения конфиденциальности информации.
15. Построение систем защиты от угрозы нарушения целостности информации.
16. Построение систем защиты от угрозы отказа доступа к информации.
17. Политика безопасности. Понятие политики безопасности. Понятия доступа и монитора безопасности. Основные типы политики безопасности.
18. Модели безопасности. Модель матрицы доступов HRU.
19. Модель распространения прав доступа Take-Grant.
20. Модель системы безопасности Белла-Лападула.
21. Основные критерии защищенности АС. Классификация систем защиты АС. Руководящие документы Государственной технической комиссии России.
22. Общие критерии (ОК). Основные положения ОК.
23. Криптографические методы защиты информации. Основные понятия криптографии. Исторические шифры.
24. Теоретическая, практическая и временная стойкость системы криптографической защиты.
25. Методы получения псевдослучайных последовательностей. Современные поточные и блочные алгоритмы шифрования.
26. Системы симметричного шифрования.
27. Системы асимметричного шифрования, открытый ключ, электронная подпись.
28. Вопросы генерации и распределения ключей. Обоснование надежности криптографической защиты.

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф – Программа вступительных испытаний		

Перечень рекомендуемой литературы:

1. Теория вероятностей. Учеб, для вузов. Вентцель Е.С. - М: Высшая школа, 1999.-575 с.
2. Теория вероятностей. Учеб, для вузов. А.В. Печинкин, О.И. Тескин, Г.М. Цветкова и др. М.: МГТУ им Н.Э Баумана, 2004 с.
3. Теоретические основы компьютерной безопасности: Учеб, пособие для вузов / П.Н. Девянин, О.О. Михальский, Д.И. Правиков и др. - М: Радио и связь. 2000.-192 с.
4. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учеб, пособие для вузов / П.Ю. Белкин, О.О. Михальский, А.С. Першаков и др. - М.: Радио и связь, 1999. - 168 с.
5. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учеб, пособие для вузов / Проскурин В.Г., Крутое СВ., Мацкевич И.В. - М: Радио и связь, 2000. -168 с.
6. Герасименко В.А. Защита информации в автоматизированных системах обработки данных: В 2-х кн.: Кн. 1. - М.: Энергоатомиздат, 1994. - 400 с.
7. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. - Феникс, 2008. -173 с.
8. Герасименко В.А., Малюк А.А. Основы защиты информации. - М: МОПО, МИФИ, 1997.-537 с.
9. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. — М.: Яхтсмен, 1996.- 192 с.
10. Теория и практика обеспечения информационной безопасности / Под ред. И. Д. Зегжды. - М.: Издательство агентства «Яхтсмен», 1996. - 192 с.
11. Хоффман Л.Дж. Современные методы защиты информации / Пер. с англ.; Под ред. В.А. Герасименко. - М.: Советское радио, 1980. - 363 с.

2.5. Шкала оценивания ответов на экзамене

неудовлетворительно	удовлетворительно	хорошо	отлично
до 39 баллов	40 - 74 баллов	75 - 84 баллов	85 - 100 баллов

Общая продолжительность экзамена составляет 45 минут.

Максимальное количество баллов за экзамен – 100. Минимальное количество баллов для успешного прохождения экзамена - 40. Поступающий, набравший менее 40 баллов за экзамен, не может быть зачислен в аспирантуру.

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф – Программа вступительных испытаний		

Таблица критериев оценки устных и письменных ответов (при наличии)

Вид деятельности		
Оценка	Балл	Уровень владения темой
неудовлетворительно	до 39	Ответ на поставленный вопрос не дан или ответ неполный, отсутствует логичность повествования или допущены существенные логические ошибки
удовлетворительно	40-74	Ответ полный, допущены не существенные логические ошибки
хорошо	75-84	Ответ логичный, конкретный, присутствуют незначительные пробелы в знаниях материала программы
отлично	85-100	Ответ полный, логичный, конкретный, без замечаний. Продемонстрированы знания материала программы, умение решать предложенные задачи

Вступительное испытание проводится экзаменационной комиссией, действующей на основании приказа ректора.

Итоговая оценка за экзамен определяется как средний балл, выставленный всеми членами комиссии.