МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

**ПРОГРАММА  
вступительного испытания**

**для поступающих в магистратуру по направлению подготовки   
10.04.01 «Информационная безопасность»**

**программа (профиль)**

**«Информационная безопасность»,**

**«Информационная безопасность цифровых технологий»**

**ОБЩИЕ ПОЛОЖЕНИЯ**

Вступительное испытание предназначено для определения практической и теоретической подготовленности поступающего в магистратуру и проводится с целью определения соответствия знаний умений и навыков требованиям обучения магистратуры по направлению подготовки 10.04.01 «Информационная безопасность» (магистратура). Программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего профессионального образования.

Вступительное испытание в магистратуру проводят экзаменационные комиссии, назначенные председателем приёмной комиссии УУНиТ.

**ПРОЦЕДУРА ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ**

Дата и время проведения вступительного испытания и консультации определяются расписанием вступительных испытаний, которое утверждается председателем приемной комиссии.

Перед вступительным испытанием для поступающих проводится консультация по содержанию программы испытания, критериям оценки, предъявляемым требованиям, правилам поведения на испытании.

Форма вступительного испытания (в соответствии Положением о вступительных испытаниях УУНИТ): тестирование.

Вступительные испытания в виде электронного тестирования проводятся в соответствии с программами вступительных испытаний, утверждаемых председателем предметной комиссии.

Вступительные испытания в форме тестирования включают вопросы как закрытого, так и открытого типа, а также задания в аудио- и видеоформатах.

Составление вариантов экзаменационных заданий в форме электронных тестов осуществляется ответственным секретарем приемной комиссии университета.

Из вариантов экзаменационных заданий формируются комплекты вопросов-тестов.

Компоновку комплектов вопросов-тестов ответственный секретарь, заместитель ответственного секретаря производят до вступительных испытаний.

Тест содержит 40 тестовых вопросов.

Результаты испытаний оцениваются по 100 бальной шкале.

Абитуриент, не согласный с оценкой, полученной на ВИ и (или) в связи с нарушением процедуры проведения ВИ имеет право подать апелляцию. Процедура подачи и рассмотрения апелляции регламентируется Положением об апелляционной комиссии УУНиТ.

**КРИТЕРИИ ОЦЕНИВАНИЯ ОТВЕТА**

Критериями оценки экзаменационного ответа, поступающего в магистратуру являются полнота, логичность, доказательность, прочность, осознанность знаний и теоретическая обоснованность суждений, самостоятельность в интерпретации информации, практическая направленность, уровень овладения профессиональными умениями и др. В случае тестирования критериями оценки являются правильные ответы на тестовые задания.

При проверке количество первичных баллов переводится в итоговую 100 балльную шкалу через информационную платформу университета.

**СОДЕРЖАНИЕ РАЗДЕЛОВ И ТЕМ ПРОГРАММЫ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ**

**Теоретические основы информационной безопасности**

1. Понятие защиты информации и информационной безопасности
2. Уязвимости информационных систем, угрозы и атаки, классификация угроз информационной безопасности
3. Риск нарушения информационной безопасности, методы анализа риска
4. Методы несанкционированного доступа к информации
5. Система защиты информации, методы защиты информации.
6. Средства информационно-технического и информационно-психологического воздействия
7. Политика безопасности на предприятии
8. Методика построения модели угроз на предприятии, модель нарушителя.

**Организационное и правовое обеспечение информационной безопасности**

1. Основные направления, принципы и условия организационной защиты информации
2. Организация службы безопасности на предприятии
3. Подбор сотрудников и работа с кадрами
4. Организация внутриобъектового режима
5. Планирование мероприятий по организационной защите информации на предприятии
6. Организация аналитической работы в области защиты информации на предприятии

**Вычислительные сети**

1. Сетевая семиуровневая модель OSI
2. Основы стека протоколов TCP/IP
3. Модуляция. Аналоговая модуляция, цифровое кодирование
4. Основы сетей LAN и WAN
5. Основы адресации и создания сетей IPv4
6. Коммутация в локальных сетях
7. Беспроводные локальные сети

**Программно-аппаратные средства защиты информации**

1. Средства криптографической защиты информации
2. Меры защиты от НСД
3. Методы защиты от несанкционированного использования и копирования
4. Компьютерные вирусы и борьба с ними

**Защита информационных процессов в компьютерных системах и сетях**

1. Защита информационных процессов в ОС семейства Windows
2. Защита информационных процессов в ОС семейства Linux
3. Реализация защищенных распределительных вычислительных систем

**Управление информационной безопасностью**

1. Защита информации как управляемая деятельность
2. Методы системного анализа для исследования сложных систем управления ИБ
3. Организация защиты информации ограниченного доступа, обрабатываемой в ИС, на основе нормативных и методических документов в сфере ИБ
4. Формирование политики ИБ как один из аспектов управления ИБ
5. Мониторинг и управление инцидентами ИБ
6. Интеллектуальная поддержка управления ИБ в ИС

**Проектирование защищенных автоматизированных систем**

1. Организация защиты инфраструктуры коммутации и маршрутизации в сети
2. Организация демилитаризованной зоны на предприятии
3. Межсетевые экраны. Принцип работы, классификация, реализация защиты.
4. Построение вычислительной сети предприятия с точки зрения архитектуры безопасности сети.

**Криптография**

1. Криптографические алгоритмы, отечественные криптографические алгоритмы
2. Симметричное и ассиметричное шифрование
3. Хэш-функции
4. Инфраструктура обмена ключами
5. Сертификаты обмена ключей

**Защищенный документооборот**

1. Обеспечение конфиденциальности документооборота
2. Системы защищенного документооборота
3. Государственная и коммерческая тайна

**Демоверсия экзаменационного варианта**

***(пробный тест)***

1. Какие свойства информации описывает модель CIA?

а) Конфиденциальность

б) Незащищенность

в) Целостность

г) Доступность

2. Что из перечисленного является носителем защищаемой информации?

а) Элементарные частицы

б) Акустические поля

в) Электромагнитные поля

г) Линии связи

1. Что позволяет сделать алгоритм Диффи-Хеллмана?

а) Выработать личные ключи пользователей и обменяться ими в результате переговоров по секретному каналу

б) Выработать общий секретный ключ в результате переговоров по прослушиваемому каналу

в) Выработать общий секретный ключ в результате переговоров по секретному каналу

г) Выработать личные ключи и обменять парными с ними открытыми ключами в результате переговоров по секретному каналу

1. Какой операции не существует в эллиптической криптографии?

а) Скалярное умножение точки

б) Умножение точек

в) Сложение точек

г) Удвоение точки

5. Расставьте в правильном порядке этапы организации защиты коммерческой тайны на предприятии.

а) Определяются аппаратные и программные средства защиты и хранения коммерческой тайны

б) Разрабатывается или перерабатывается политика безопасности предприятия

в) Обеспечивается ИБ на основе взаимодействия между всеми структурными подразделениями предприятия

г) Принимается Положение по обеспечению сохранности коммерческой тайны

д) Осуществляется аудит и независимая оценка сведений и объектов, нуждающихся в защите на предприятии, и осуществляется постоянное совершенствование мер защиты еще до внедрения

**СПИСОК ЛИТЕРАТУРЫ**

1. Управление безопасностью [Текст] : учеб. пособие / Л. П. Гончаренко, Е. С. Куценко; Рос. экон. акад. им. Г. В. Плеханова.- М.: КноРус, 2010.-272 с.
2. Информационная безопасность и защита информации [Текст] : учеб. пособие / В. П. Мельников и др.; под ред. С. А. Клейменова.- М. : Академия , 2009.-330 с.
3. Информационная безопасность региона : традиции и инновации [Текст] : монография / Л. В. Астахова и др.; под науч. ред. Л. В. Астаховой ; Юж.-Урал. гос. ун-т, Каф. Информ. безопасность; ЮУрГУ.- Челябинск: Издательский Центр ЮУрГУ , 2009.-268 с.
4. Галатенко, В. А. Основы информационной безопасности : Курс лекций: Учеб. пособие для вузов по специальностям в обл. информ. технологий / В. А. Галатенко; Под ред. В. Б. Бетелина; Интернет-ун-т информ. технологий.- . : Интернет-Университет Информационных Технологий , 2006.-205 с.
5. Аникин П.П., Балыбердин А.Л., Вус М.А. Государственная тайна и ее защита в Российской Федерации: учеб. пособие (под ред. Вуса М.А., Федорова А.В.; предисл. Кропачева Н.М., Сидоровой Н.А.). – Изд. 2-е, перераб., доп. –изд-во Р. Асланова «Юридический Центр-Пресс«, 2005. – 623 с. – 1 050 экз.
6. Анин Б.Ю. Защита компьютерной информации. – БХВ-Петербург, 2000. – 384 с. – 7 000 экз.
7. Семкин С.Н., Беляков Э.В., Гребенев С.В., Козачок В.И. «Основы организационного обеспечения информационной безопасности объектов информатизации». – М.: Гелиос АРВ, 2010.
8. Программно-аппаратная защита информации [Текст] : учеб. пособие по направлениям "Информ. безопасность" и "Информатика и вычисл. техника" / П. Б. Хорев.- М. : Форум , 2009.-351 с.
9. Кибербезопасность: правила игры : как руководители и сотрудники влияют на культуру безопасности в компании / Эллисон Сэрра ; перевод с английского: [Людмила Смилевска]. - Москва : Сбер : Альпина ПРО, 2021.
10. Аудит информационной безопасности автоматизированных систем : учебное пособие / В. А. Воеводин, А. А. Хорев ; под редакцией А. А. Хорева Министерство науки и высшего образования Российской Федерации, Национальный исследовательский университет "МИЭТ". - Москва : МИЭТ, 2021.
11. Теория информации / Р. Л. Стратонович. - Изд. 2-е. - Москва : URSS : ЛЕНАНД, 2021.
12. Актуальные вопросы правового регулирования и защиты информации в России : избранные труды / В. А. Северин. - Москва : URSS : Ленанд, 2022 [т. е. 2021]. - 474 с.
13. Старший брат следит за тобой : как защитиь себя в цифровом мире / Михаил Райтман. - Москва : Альпина Паблишер, 2022.
14. Проблемы правовой и технической защиты информации : [сборник статей / АлтГУ] ; редакционная коллегия: Поляков В.В., проф., д.ф.-м.н. - главный редактор [и др.]. - Барнаул : Изд-во Алтайского государственного университета, 2021.
15. Глоссарий официальных дефиниций в сфере информации, информационных технологий и защиты информации : словарь-справочник / А.В. Парамонов, И.А. Коннов ; Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Нижегородский институт управления. - Нижний Новгород : Дятловы горы, 2021.
16. Киберзащита автоматизированных систем воинских формирований : монография / А. А. Бойко. - Санкт-Петербург : Наукоемкие технологии, 2021.
17. Безопасность в беспроводных корпоративных сетях : монография / Корягина С. А. - Москва : National Research, 2021.