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»

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): устно-письменная (с элементами тестирования).

Вступительные испытания в виде устного с элементами тестирования проводятся в соответствии с программами вступительных испытаний, утверждаемых председателем приемной комиссии.

Экзаменационные билеты включают тестовые задания и один вопрос по направлению подготовки магистратуры.

В аудитории, где проводится вступительное испытание в устной форме, не может находиться одновременно более 12 человек. Нахождение в аудитории посторонних лиц не допускается.

Абитуриенту предоставляется право готовиться к ответу в течение 20 минут.

Абитуриенту предоставляется право ответа на экзаменационные вопросы в течение 10 минут.

В процессе сдачи вступительного испытания абитуриенту могут быть заданы дополнительные вопросы как по содержанию экзаменационного билета, так и по любым разделам предмета в пределах программы вступительного испытания.

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 менеджера и др. В случае тестирования является правильные ответы на тестовые задания.

Результаты экзамена определяются по 100-балльной шкале, за тестовую часть можно получить максимально 40 баллов (10 вопросов по 4 балла), за устный ответ комиссии 60 баллов. Разброс баллов представлен ниже в таблице:

№	*Критерии оценивания*	*Оценка*
1	Дан полный развернутый ответ на теоретический вопрос: грамотно использована научная терминология; – четко сформулирована проблема, доказательно аргументированы выдвигаемые тезисы; – указаны основные точки зрения, принятые в научной литературе по рассматриваемому вопросу; – аргументирована собственная позиция или точка зрения, обозначены наиболее значимые в данной области научно-исследовательские проблемы. Тестовая часть вопроса написана на 40-32 балла.	85-100 баллов «отлично»
2	Дан в целом правильный ответ на теоретический вопрос: – применяется научная терминология, но при этом допущена ошибка или неточность в определениях, понятиях; – проблема сформулирована, в целом доказательно аргументированы выдвигаемые тезисы; – имеются недостатки в аргументации, допущены фактические или терминологические неточности, которые не носят существенного характера; – высказано представление о возможных научно-исследовательских проблемах в данной области. Тестовая часть написана на 32-20 баллов.	67-84 балла «хорошо»
3	Дан в основном правильный ответ на теоретическийвопрос: – названы и определены лишь некоторые основания, признаки, характеристики рассматриваемой проблемы; – допущены существенные фактические и (или) терминологические неточности; – собственная точка зрения недостаточно полно аргументирована; – не высказано представление о возможных научно-исследовательских проблемах в данной области. Тестовая часть написана на 20-16 баллов.	50-66 баллов «удовлетворительно»

4	Дан фрагментарный ответ или неправильный ответ на теоретический вопрос из предложенного тематического раздела: – отмечается отсутствие знания терминологии, научных оснований, признаков, характеристик рассматриваемой проблемы; – собственная точка зрения по данному вопросу не представлена. Тестовая часть написана на 16-0 баллов.	0-49 баллов «неудовлетвори тельно»

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. Организация охраны объекта
6. Организация пропускного режима
7. Планирование мероприятий по организационной защите информации на предприятии
8. 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. Маршрутизация IPv4
7. Коммутация в локальных сетях
8. 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. Стадии проектирования защищенных автоматизированных систем
2. Проектирование системы защиты информации в соответствии с нормативной правовой базой РФ (на примере ИСПДн, ГИС или ЗОКИИ)
3. Организация защиты инфраструктуры коммутации и маршрутизации в сети
4. Организация демилитаризованной зоны на предприятии
5. Межсетевые экраны. Принцип работы, классификация, реализация защиты.
6. Средства антивирусной защиты. Принцип работы, классификация, реализация защиты.
7. Системы обнаружения вторжений. Принцип работы, классификация, реализация защиты.
8. SIEM и DLP-системы. Принцип работы, классификация, реализация защиты.

ДЕМОВЕРСИЯ ЭКЗАМЕНАЦИОННОГО ВАРИАНТА

1. Тестовая часть билета

1. Согласно какому нормативному документу выбираются меры и требования для проектирования системы защиты информации значимых объектов КИИ?

а) Федеральный закон №152-ФЗ «О безопасности персональных данных» от 27.07.2006

б) Федеральный закон №187-ФЗ «О безопасности критической информационной инфраструктуры РФ» от 26.07.2017

в) Постановление правительства от 8 февраля 2018 г. №127 «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»

г) Приказ ФСТЭК от 25 декабря 2017 г. №239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

Ответ:

2. Расставьте в правильном порядке стадии определения списка требований для системы защиты информации:

а) Составление уточненного набора мер и требований

б) Определение базового набора требований защиты объекта

в) Дополнение уточненного набора мер и требований

г) Составление адаптированного набора мер и требований

Ответ:

3. ….

…

10.

2. Вопрос для устного ответа

Защита информационных процессов в ОС семейства Linux

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 защитить 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.