

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ИНГУШСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФИЗИКО- МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра «Информационные системы и технологии»**

СОГЛАСОВАНО

Руководитель образовательной программы

_____/М.Х.Мальсагов
от «03» марта 2025г.

УТВЕРЖДАЮ

И.о. декана физико-математического
факультета

_____/Б.С.Кульбужев
от «14» марта 2025г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.17 Угрозы информационной безопасности, анализ и обнаружения атак

Направление подготовки

09.03.02 Информационные системы и технологии

-

Направленность (профиль подготовки)

Безопасность информационных систем

Квалификация выпускника

Бакалавр

Форма обучения

Очная, очно-заочная

Магас, 2025

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Целью освоения дисциплины **«Информационная безопасность и защита информации»** является:

- изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

1.2. Изучение дисциплины **«Информационная защита и безопасность»** способствует решению следующих задач профессиональной деятельности

- изучение концепции инженерно-технической защиты информации;
- изучение теоретических основ инженерно - технической защиты информации;
- изучение физических основ инженерно-технической защиты информации;
- изучение технических средств добывания и защиты информации;
- изучение организационных основ инженерно-технической защиты информации;
- изучение методического обеспечения инженерно-технической защиты информации.

1.3. Процесс изучения дисциплины направлен на формирование следующих компетенций:

общепрофессиональные (ОПК)

Код компетенции	Наименование и (или) описание компетенции
	пониманием сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны

профессиональные (ПК)

Код компетенции	Наименование и (или) описание компетенции
	способностью обеспечивать безопасность и целостность данных информационных систем и технологий

1.4. В результате освоения дисциплины обучающийся должен:

- **Знать:** средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации;
- **Уметь:** пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения;
- **Владеть:** методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Предшествующими дисциплинами учебного плана являются: Методы и средства проектирования информационных систем и технологий, Проектирование информационных систем управления, Администрирование информационных систем управления

№ п/п	Наименование разделов и тем дисциплины (модуля)	семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)								Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации (по семестрам)							
			Контактная работа					Самостоятельна я работа										
			Всего	Лекции	Практические занятия	Лабораторные занятия	Др. виды контакт. работы	Всего	Курсовая работа(проект)	Подготовка к экзамену	Другие виды самостоятельной работы	Собеседование	Коллоквиум	Проверка тестов	Проверка контрольн. работ	Проверка реферата	Проверка эссе и иных творческих работ	курсовая работа (проект) др.
	Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.			10	10	8				8								
	Три вида возможных нарушений информационной системы. Защита. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.			4	4	6				7								

Таксономия нарушений информационной безопасности вычислительной системы. Использование защищенных компьютерных систем.			4	4	4					3							
Всего			18	18	18					18							
Курсовая работа (проект)																	
Подготовка к экзамену																	
Общая трудоемкость, в часах		72	18	18	18					18	Промежуточная						
											Форма						
											Зачет						*
											Зачет с оценкой						
											Экзамен						

3. СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Модуль 1. Основопологающие положения

Тема 1.1. Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей.

Стандарты в области информационной безопасности. Международные стандарты информационного обмена. Понятие угрозы, атаки. Глобальные сети и информационная безопасность.

Виды учебных занятий:

Лекция: Международные стандарты информационного обмена.
Понятие угрозы. Информационная
безопасность в условиях функционирования в России
глобальных сетей.

Тема 1.2. Виды противников или «нарушителей». Понятие о видах вирусов.

Понятие нарушителя информационной безопасности. Хакеры. Виды хакеров. Примеры хакерских атак. Вирусы как класс вредоносного программного обеспечения. Виды вирусов и их классификация.

Виды учебных занятий:

Лекция: Виды противников или «нарушителей».
Понятие о видах вирусов.

Тема 1.3. Три вида возможных нарушений информационной системы. Защита

Три вида возможных нарушений информационной безопасности. 3 составляющих ИБ - целостность, доступность, конфиденциальность. Защита информационной системы от угроз.

Виды учебных занятий:

Лекция: Три вида возможных нарушений
информационной системы. Защита.

Тема 1.4. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.

Понятие государственной, коммерческой, личной тайны. Основные нормативные документы в этой области. Рассекречивание документов. Уровень тайны.

Виды учебных занятий:

Лекция: Основные нормативные руководящие
документы, касающиеся государственной тайны,
нормативно-справочные документы

Модуль 2. Основные положения теории информационной безопасности

Тема 2.1. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.

Схема построения информационной безопасности на уровне государства. Назначение и задачи в сфере обеспечения безопасности. Специальные отделы и их функции в процессе обеспечения информационной безопасности государства. Военные подразделения в сфере информационной безопасности.

Виды учебных занятий:

Лекция:	Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства
---------	---

Тема 2.2. Основные положения теории информационной безопасности. Модели безопасности и их применение.

Основные положения теории информационной безопасности. Анализ различных моделей безопасности, как для крупного объекта, так и для относительно небольшой компании. Модели безопасности для домашней информационной системы. Применение методов информационной безопасности.

Виды учебных занятий:

Лекция:	Основные положения теории информационной безопасности. Модели безопасности и их применение.
---------	---

Тема 2.3. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.

Понятие таксономии нарушения безопасности. Причины нарушения информационной безопасности. Аудит событий в рамках информационной системы.

Виды учебных занятий:

Лекция:	Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование
Практическое занятие:	Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование

Тема 2.4. Анализ способов нарушений информационной безопасности.

Анализ различных способов нарушений информационной безопасности. Хакерские атаки, отказы оборудования в обслуживании, внешние факторы, влияющие прямо на информационную безопасность систем.

Виды учебных занятий:

- Лекция: Анализ способов нарушений информационной безопасности.
- Практическое занятие: Анализ способов нарушений информационной безопасности.

Модуль 3. Защита информации

Тема 3.1. Использование защищенных компьютерных систем.

Защищенные компьютерные системы. Их виды и особенности. Примеры защищенных систем. Их использование и применение на практике.

Виды учебных занятий:

- Лекция: Использование защищенных компьютерных систем.

Тема 3.2. Методы криптографии

Криптография, Криптоанализ. Основные понятия криптологии. История шифрования. Использование шифрования различными методами. Рассмотрение сокрытия информации таблицей Винжера. Программы для криптографии. Электронная цифровая подпись.

Виды учебных занятий:

- Лекция: Методы криптографии.
- Практическое занятие: Методы криптографии.

Тема 3.3. Основные технологии построения защищенных систем.

Основные технологии построения защищенных систем. Физические устройства. Их виды и использование. Программные пакеты. Виды программных пакетов для обеспечения защищенной системы. Правовые особенности использования средств информационной защиты.

Виды учебных занятий:

- Лекция: Основные технологии построения защищенных систем
- Практическое занятие: Основные технологии построения защищенных систем.

Тема 3.4. Место информационной безопасности экономических систем в национальной безопасности страны

Информационная безопасность страны. Защита экономических систем. Обмен конфиденциальной информацией. Структура банковских информационных систем в области защиты информации. Важность защиты экономических систем. Электронные деньги и безопасность финансовых переводов. Концепция информационной безопасности. Основные сведения и положения.

Виды учебных занятий:

Лекция: Место информационной безопасности экономических систем в национальной безопасности страны

4. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

4.1. Темы контрольных работ

- 1 Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними
- 2 Современные средства защиты информации
- 3 Современные системы компьютерной безопасности
- 4 Современные средства противодействия экономическому шпионажу
- 5 Современные криптографические системы
- 6 Криптоанализ, современное состояние
- 7 Правовые основы защиты информации
- 8 Технические аспекты обеспечения защиты информации. Современное состояние
- 9 Атаки на систему безопасности и современные методы защиты
- 10 Современные пути решения проблемы информационной безопасности РФ

4.2. Тематика курсовых работ (проектов)

Рабочим учебным планом выполнение курсовой работы (проекта) не предусмотрено.

4.3. Перечень методических рекомендаций

№ п/п	Наименование
1	Методические рекомендации по выполнению контрольной работы

4.4. Перечень вопросов для подготовки к экзамену

1. Что такое информационная безопасность?
2. Какие предпосылки и цели обеспечения информационной безопасности?
3. В чем заключаются национальные интересы РФ в информационной сфере?
4. Что включает в себя информационная борьба?
5. Какие пути решения проблем информационной безопасности РФ существуют?
6. Каковы общие принципы обеспечения защиты информации?
7. Какие имеются виды угроз информационной безопасности предприятия (организации)?
8. Какие источники наиболее распространенных угроз информационной безопасности существуют?
9. Какие виды сетевых атак имеются?
10. Какими способами снизить угрозу спуфинга пакетов?
11. Какие меры по устранению угрозы IP -спуфинга существуют?
12. Что включает борьба с атаками на уровне приложений?
13. Какие существуют проблемы обеспечения безопасности локальных вычислительных сетей?
14. В чем заключается распределенное хранение файлов?
15. Что включают в себя требования по обеспечению комплексной системы информационной безопасности?
16. Какие уровни информационной защиты существуют, их основные составляющие?
17. В чем заключаются задачи криптографии?
18. Зачем нужны ключи?
19. Какая схема шифрования называется многоалфавитной подстановкой?
20. Какие системы шифрования вы знаете?
21. Что включает в себя защита информации от несанкционированного доступа?
22. В чем заключаются достоинства и недостатки программно-аппаратных средств защиты информации?
23. Какие виды механизмов защиты могут быть реализованы для обеспечения идентификации и аутентификации пользователей?
24. Какие задачи выполняет подсистема управления доступом?
25. Какие требования предъявляются к подсистеме протоколирования аудита?
26. Какие виды механизмов защиты могут быть реализованы для обеспечения конфиденциальности данных и сообщений?
27. В чем заключается контроль участников взаимодействия?
28. Какие функции выполняет служба регистрации и наблюдения?
29. Что такое информационно-опасные сигналы, их основные параметры?

30. Какие требования необходимо выполнять при экранировании помещений, предназначенных для размещения вычислительной техники?
31. Какой процесс называется аутентификацией пользователя?
32. Какие схемы аутентификации вы знаете?
33. Что такое смарт-карты?
34. Какие требования предъявляются к современным криптографическим системам защиты информации?
35. Что такое симметричная криптосистема?
36. Какие виды симметричных криптосистем существуют?
37. Что такое асимметричная криптосистема?
38. Что понимается под односторонней функцией?
39. Как классифицируются криптографические алгоритмы по стойкости?
40. В чем заключается анализ надежности криптосистем?
41. Что такое дифференциальный криптоанализ?
42. В чем сущность криптоанализа со связанными ключами?
43. В чем сущность линейного криптоанализа?
44. Какие атаки изнутри вы знаете?
45. Какая программа называется логической бомбой?
46. Какими способами можно проверить систему безопасности?
47. Что является основными характеристиками технических средств защиты информации?
48. Какие требования предъявляются к автоматизированным системам защиты третьей группы?
49. Какие требования предъявляются к автоматизированным системам защиты второй группы?
50. Какие требования предъявляются к автоматизированным системам защиты первой группы?
51. Какие классы защиты информации от несанкционированного доступа для средств вычислительной техники имеются? От чего зависит выбор класса защищенности?
52. Какие требования предъявляются к межсетевым экранам?
53. Какие имеются показатели защищенности межсетевых экранов?
54. Какие атаки системы снаружи вы знаете?
55. Какая программа называется вирусом?
56. Какая атака называется атакой отказа в обслуживании?
57. Какие виды вирусов вы знаете?
58. Какие вирусы называются паразитическими?
59. Как распространяются вирусы?
60. Какие методы обнаружения вирусов вы знаете?
61. Какая программа называется монитором обращения?
62. Что представляет собой домен?
63. Как осуществляется защита при помощи ACL -списков?
64. Какой список называется перечнем возможностей?
65. Какие способы защиты перечней возможностей вы знаете?

66. Из чего состоит высоконадежная вычислительная база (ТСВ)?
67. Какие модели многоуровневой защиты вы знаете?
68. В чем заключается организация работ по защите от несанкционированного доступа интегрированной информационной системы управления предприятием?
69. Какие характеристики положены в основу системы классификации информационных систем управления предприятием?
70. Какие задачи решает система компьютерной безопасности?
71. Какие пути защиты информации в локальной сети существуют?
72. Какие задачи решают технические средства противодействия экономическому шпионажу?
73. Какой порядок организации системы видеонаблюдения?
74. Что включает в себя защита информационных систем с помощью планирования?
75. Какие условия работы оцениваются при планировании?
76. Из каких этапов состоят работы по обеспечению информационной безопасности предприятия?
77. Что такое мобильные программы?
78. Что такое концепция потоков?
79. Что представляет собой метод «песочниц»?
80. Что такое интерпретация?
81. Что такое программы с подписями?
82. Что представляет собой безопасность в системе Java ?
83. Назовите несколько примеров политик безопасности пакета JDK 1.2?
84. Какие международные документы регламентируют деятельность по обеспечению защиты информации?
85. Что понимают под политикой информационной безопасности?
86. Что включает в себя политика информационной безопасности РФ?
87. Какие нормативные документы РФ определяют концепцию защиты информации?

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине по решению кафедры оформлен отдельным приложением к рабочей программе.

6. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Основная литература:

1. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. Текстовые данные.— Саратов: Профобразование, 2017.— 544 с.— Режим доступа: <http://www.iprbookshop.ru/63592.html>.
2. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс]: лабораторный практикум/ М.А. Лапина [и др.].— Электрон. текстовые данные.— Ставрополь: Северо- Кавказский федеральный университет, 2016.— 242 с.— Режим доступа: <http://www.iprbookshop.ru/62945.html>.
3. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаши А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: <http://www.iprbookshop.ru/10677.html>.
4. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИБ), 2014.— 256 с.— Режим доступа: <http://www.iprbookshop.ru/33430.html>.

Дополнительная литература:

1. Основы информационной безопасности : опорный конспект / Е.А. Рыбакова. - СПб.: Изд-во СЗТУ, 2016. - 49 с.
2. Васильев В.И. Интеллектуальные системы защиты информации [Электронный ресурс]: учебное пособие/ Васильев В.И.— Электрон. Текстовые данные.— М.: Машиностроение, 2013.— 172 с.— Режим доступа: <http://www.iprbookshop.ru/18519.html>.
3. Инструментальный контроль и защита информации [Электронный ресурс]: учебное пособие/ Н.А. Свиначев [и др.].— Электрон. Текстовые данные.— Воронеж: Воронежский государственный университет инженерных технологий, 2013.— 192 с.—
Режим доступа: <http://www.iprbookshop.ru/47422.html>.
4. Калмыков И.А. Криптографические методы защиты информации [Электронный ресурс]: лабораторный практикум/ Калмыков И.А., Науменко Д.О., Гиш Т.А.— Электрон. Текстовые данные.— Ставрополь: Северо- Кавказский федеральный университет, 2015.— 109 с.— Режим доступа: <http://www.iprbookshop.ru/63099.html>.
5. Пашинцев В.П. Нестандартные методы защиты информации [Электронный ресурс]: лабораторный практикум/ Пашинцев В.П., Ляхов А.В.— Электрон. Текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2016.— 196 с.—
Режим доступа: <http://www.iprbookshop.ru/63217.html>.

6. Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс]/ Петров А.А.— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 446 с.— Режим доступа: <http://www.iprbookshop.ru/63800.html>.

7. Нестеров С.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие/ Нестеров С.А.— Электрон. текстовые данные.— СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2014.— 322 с.— Режим доступа: <http://www.iprbookshop.ru/43960.html>. **Программное обеспечение**

1. ППП MS Office 2010
2. Текстовый редактор Блокнот
3. Браузеры IE, Google Chrome, Opera и др.

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО – ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Электронная информационно-образовательная среда АНО ВПО "СЗТУ" (ЭИОС СЗТУ) [Электронный ресурс]. - Режим доступа: <http://edu.nwotu.ru/>
2. Электронная библиотека АНО ВПО "СЗТУ" [Электронный ресурс]. - Режим доступа: <http://lib.nwotu.ru:8087/jirbis2/>
3. Электронно-библиотечная система IPRbooks [Электронный ресурс]. - Режим доступа: <http://www.iprbookshop.ru/>
4. Информационная система "Единое окно доступа к образовательным ресурсам" [Электронный ресурс]. - Режим доступа: <http://window.edu.ru/>
5. Информационная системы доступа к электронным каталогам библиотек сферы образования и науки (ИС ЭКБСОН) [Электронный ресурс]. - Режим доступа: <http://www.vlibrary.ru/>

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

9.1 Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, практические занятия, контрольную работу, самостоятельную работу студента, консультации.

9.2. После изучения каждого модуля дисциплины необходимо ответить на вопросы контрольного теста по данному модулю с целью оценивания знаний и получения баллов.

9.3. При изучении модулей 1 - 3 необходимо выполнить задания контрольной работы, руководствуясь методическими рекомендациями по ее выполнению.

9.4. По завершению изучения Модулей 1 – 3 учебной дисциплины в седьмом семестре студент обязан пройти промежуточную аттестацию. Вид промежуточной аттестации определяется рабочим учебным планом. Форма проведения промежуточной аттестации – компьютерное тестирование с использованием автоматизированной системы тестирования знаний студентов в ЭИОС.

9.5. К промежуточной аттестации допускаются студенты, выполнившие требования рабочего учебного плана.

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

При осуществлении образовательного процесса по дисциплине используются следующие информационные технологии:

10.1. Internet – технологии:

(WWW(англ. World Wide Web – Всемирная Паутина) – технология работы в сети с гипертекстами;

FTP (англ. File Transfer Protocol – протокол передачи файлов) – технология передачи по сети файлов произвольного формата;

IRC (англ. Internet Relay Chat – поочередный разговор в сети, чат) – технология ведения переговоров в реальном масштабе времени, дающая возможность разговаривать с другими людьми по сети в режиме прямого диалога;

ICQ (англ. I seek you – я ищу тебя, можно записать тремя указанными буквами) – технология ведения переговоров один на один в синхронном режиме.

10.2. Дистанционное обучение с использованием ЭИОС на платформе Moodle.

- Технология мультимедиа в режиме диалога.
- Технология неконтактного информационного взаимодействия (виртуальные кабинеты, лаборатории).
- Гипертекстовая технология (электронные учебники, справочники, словари, энциклопедии).

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

1. Библиотека.
2. Справочно-правовая система Консультант Плюс.
3. Электронная информационно-образовательная среда университета.
4. Локальная сеть с выходом в Интернет.

12. БАЛЛЬНО-РЕЙТИНГОВАЯ СИСТЕМА

Формирование оценки текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины осуществляется с использованием балльно-рейтинговой оценки работы студента.

Вид учебной работы, за которую ставятся баллы	баллы
Участие в online занятиях, прослушивание видео лекций	0 – 5
Контрольный тест 1	0 – 15
Контрольный тест 2	0 – 15
Контрольный тест 3	0 – 15
Контрольная работа	0 – 20
Промежуточная аттестация (итоговый контрольный тест)	0 – 30
Всего	0 - 100

БОНУСЫ (баллы, которые могут быть добавлены до 100)	Баллы
- за активность	0-10
- за участие в олимпиаде	0-50
- за участие в НИРС	0-50
- за оформление заявок на полезные методы (рац. предложения)	0-50

Балльная шкала оценки

Оценка (экзамен)	Баллы
отлично	86 – 100
хорошо	69 – 85
удовлетворительно	51 – 68
неудовлетворительно	менее 51

Оценка по контрольной работе

Оценка	Количество баллов
отлично	18 - 20
хорошо	15 - 17
удовлетворительно	12 - 14
неудовлетворительно	менее 12

Сведения о переутверждении программы на очередной учебный год и регистрации изменений

Учебный год	Решение кафедры (№ протокола, дата)	Внесенные изменения	Подпись зав. кафедрой

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ (МОДУЛЯ)

**Б1.В.17 Угрозы информационной безопасности, анализ и
обнаружения атак**

Направление подготовки

09.03.02 Информационные системы и технологии

-

Направленность (профиль подготовки)

Безопасность информационных систем

Квалификация выпускника

Бакалавр

Форма обучения

Очная, заочная

Магас, 2025

1. Показатели и критерии оценивания компетенций по этапам формирования

Этапы освоения компетенции	Показатели достижения заданного уровня освоения компетенций	Критерии оценивания результатов обучения				
		1	2	3	4	5
Первый этап	Знать (ОПК-4, ПК-31) - средства и методы предотвращения и обнаружения вторжений; - технические каналы утечки информации; - возможности технических средств перехвата информации; - способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - организацию защиты информации от утечки по техническим каналам на объектах информатизации;	Не знает	Знает: средства и методы предотвращения и обнаружения вторжений; технических каналы утечки информации; Не знает: возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим	Знает: средства и методы предотвращения и обнаружения вторжений; технических каналы утечки информации; возможности технических средств перехвата информации; Не знает: способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим	Знает: средства и методы предотвращения и обнаружения вторжений; технических каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; Не знает: организацию защиты информации от утечки по техническим	Знает: средства и методы предотвращения и обнаружения вторжений; технических каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; Не знает: организацию защиты информации от утечки по техническим

			каналам на объектах информатизации;	каналам на объектах информатизации	каналам на объектах информатизации;	каналам на объектах информатизации;
Второй этап	Уметь (ОПК-4, ПК-31) - пользоваться нормативными документами по противодействию технической разведке; - оценивать качество готового программного обеспечения;	Не умеет	Практически не умеет: пользоваться нормативными документами по противодействию технической разведке; Не умеет: оценивать качество готового программного обеспечения;	Умеет: пользоваться нормативными документами по противодействию технической разведке; Не умеет: оценивать качество готового программного обеспечения;	Умеет: пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения, но может ошибиться	Умеет: пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения;
Третьй этап	Владеть (ОПК-4, ПК-31) - методами и средствами технической защиты информации; - методами расчета и инструментального контроля показателей технической защиты информации.	Не владеет	Владеет: некоторыми методами и средствами технической защиты информации; Не владеет: методами расчета и инструментального контроля показателей технической защиты информации.	Владеет: - методами и средствами технической защиты информации Не владеет: методами расчета и инструментального контроля показателей технической защиты информации.	Владеет: методами и средствами технической защиты информации; некоторыми методами расчета и инструментального контроля показателей технической защиты информации.	Владеет: методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации.

2. Шкалы оценивания

(балльно-рейтинговая система)

Вид учебной работы, за которую ставятся баллы	баллы
Участие в online занятиях, прослушивание видео лекций	0 – 5
Контрольный тест 1	0 – 15

Контрольный тест 2	0 – 15
Контрольный тест 3	0 – 15
Контрольная работа	0 – 20
Промежуточная аттестация (итоговый контрольный тест)	0 – 30
Всего	0 - 100

Балльная шкала оценки

Оценка (экзамен)	Баллы
отлично	86 – 100
хорошо	69 – 85
удовлетворительно	51 – 68
неудовлетворительно	менее 51

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций при изучении учебной дисциплины в процессе освоения образовательной программы

3.1. Типовой вариант задания на контрольную работу

Контрольная работа выполняется в форме реферата по заданной теме, оформляется на сброшюрованных листах формата А4 и представляется преподавателю в установленный срок. Студент выбирает номер темы по сумме последней и предпоследней цифр шифра. Если сумма цифр равна нулю, то выбирается тема № 10.

Перечень тем рефератов:

1. Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними
2. Современные средства защиты информации
3. Современные системы компьютерной безопасности
4. Современные средства противодействия экономическому шпионажу
5. Современные криптографические системы

6. Криптоанализ, современное состояние
7. Правовые основы защиты информации
8. Технические аспекты обеспечения защиты информации. Современное состояние
9. Атаки на систему безопасности и современные методы защиты
10. Современные пути решения проблемы информационной безопасности РФ

3.2. Типовой тест промежуточной аттестации

1. Программа, которая может размножаться, присоединяя свой код к другой программе, называется

Выберите один ответ.

- a. Компилятор
- b. Интернет-черви
- c. Вирус

2. Величиной (размером) ущерба (вреда), ожидаемого в результате несанкционированного доступа к информации или нарушения доступности информационной системы, называется

Выберите один ответ.

- a. Воздействием (влиянием)
- b. Потерей
- c. Силой

3. Код, способный самостоятельно, то есть без внедрения в другие программы, вызвать распространение своих копий по информационной системе и их выполнение, называется

Выберите один ответ.

- a. Троянской программой
- b. Червем
- c. Вирусом

4. Уровень риска, который считается доступным для достижения желаемого результата, называется

Выберите один ответ.

- a. Устойчивостью
- b. Терпимостью по отношению к риску
- c. Независимостью

5. Компьютер с одним процессором в каждый конкретный момент времени может выполнять команд

Выберите один ответ.

- a. Две
- b. Одну
- c. Сколько зададут

6. Алгоритмы реального времени, заранее назначающие каждому процессу фиксированный приоритет, после чего выполняющие приоритетное планирование с переключениями, называются:

Выберите один ответ.

- a. Статическими алгоритмами
- b. Алгоритмы RMS
- c. Динамическими алгоритмами

7. Системные файлы, обеспечивающие поддержку структур файловой системы, называются:

Выберите один ответ.

- a. Каталоги
- b. Символьные файлы
- c. Регулярные файлы

8. Коды, обладающие способностью к распространению (возможно, с изменениями) путем внедрения в другие программы, называются

Выберите один ответ.

- a. Вирусами
- b. Руткитами
- c. Червями

9. Требованием к информационной системе, являющимся следствием действующего законодательства, миссии и потребностей организации, называется:

Выберите один ответ.

- a. Правилами безопасности
- b. Требованием безопасности
- c. Мерами безопасности

10. Процессом идентификации рисков применительно к безопасности информационной системы, определения вероятности их осуществления и потенциального воздействия, а также дополнительный контрмер, ослабляющий (уменьшающий) это воздействие, называется:

Выберите один ответ.

- a. Управление риском
- b. Предупреждением рисков
- c. Анализом рисков

11. Компьютерная система, в которой два или более центральных процессоров делят полный доступ к общей оперативной памяти, называется

Выберите один ответ.

- a. Мультипроцессоры типа «хозяин-подчиненный»
- b. Симметричный мультипроцессор
- c. Мультипроцессор с общей памятью

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

4.1. Итоговый контрольный тест доступен студенту только во время тестирования, согласно расписания занятий или в установленное деканатом время.

4.2. Студент информируется о результатах текущей успеваемости.

4.3. Студент получает информацию о текущей успеваемости, начислении бонусных баллов и допуске к процедуре итогового тестирования от преподавателя или в ЭИОС.

4.4. Производится идентификация личности студента.

4.5. Студентам, допущенным к промежуточной аттестации, открывается итоговый контрольный тест.

4.6. Тест закрывается студентом лично по завершении тестирования или автоматически по истечении времени тестирования.

