

**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.11 Основы и стандарты информационной безопасности**

**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. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Категория (группа) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Наименование показателя оценивания результата обучения по дисциплине
Понимание принципов работы современных информационных технологий	<b>ОПК-2</b> Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности	<b>ОПК-2.1</b> Понимает принципы работы современных информационных технологий и программных средств, в том числе отечественного производства	Знание, умение
		<b>ОПК-2.2</b> Использует современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности	Знание, умение
Решение стандартных задач профессиональной деятельности	<b>ОПК-3</b> Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	<b>ОПК-3.2</b> Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Знание, умение, навыки
		<b>ОПК-3.3</b> Подготавливает обзоры, аннотации, рефераты научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	Знание, умение, навыки

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

**1. Компетенция ОПК-2** Способен понимать принципы работы современных информационных технологий и программных средств, в том числе

отечественного производства, и использовать их при решении задач профессиональной деятельности

Данная компетенция формируется следующими дисциплинами.

Стадия	Наименования дисциплины
1.	Информатика.
2.	Основы информационной безопасности.
3.	Вычислительная математика.
4.	Базы данных.
5.	Операционные системы.
6.	Учебная ознакомительная практика
7.	Производственная технологическая (проектно-технологическая) практика

**2. Компетенция ОПК-3** Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Данная компетенция формируется следующими дисциплинами.

Стадия	Наименования дисциплины
1.	Основы информационной безопасности.
2.	Информатика.
3.	Учебная ознакомительная практика

### 3. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 3 зач. единиц, 108 часов.

Дисциплина реализуется в рамках практической подготовки: 2 зач. единиц.

Форма промежуточной аттестации: *зачет*.

Вид учебной работы	Всего часов	Семестр №5

Общая трудоемкость дисциплины, час	108	108
<b>Контактная работа (аудиторные занятия), в т.ч.:</b>	56	56
лекции	14	14
лабораторные	56	56
практические		
групповые консультации в период теоретического обучения и промежуточной аттестации		
контроль самостоятельной работы	-	-
<b>Самостоятельная работа студентов, включая индивидуальные и групповые консультации, в том числе:</b>	38	38
Курсовой проект	-	-
Курсовая работа	-	-
Расчетно-графическое задания	-	-
Индивидуальное домашнее задание	-	-
Самостоятельная работа на подготовку к аудиторным занятиям (лекции, практические занятия, лабораторные занятия)	38	38
Зачет	-	-

#### 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

##### 4.1 Наименование тем, их содержание и объем

##### Курс 3 Семестр 5

No п/	Наименование раздела (краткое содержание)	Объем на тематический раздел по видам учебной нагрузки, час
----------	---	--

		Л е к ц и и	Практ. и и сем		Смостоят раб
1. Основные понятия информационной безопасности.					
	Актуальность проблем информационной безопасности. Основные термины и определения в области информационной безопасности. Информация. Классификация информации. Общий порядок работы с информацией, отнесенной к категории конфиденциальная информация. Аспекты информационной безопасности. Понятие комплексной защиты информации.	3	4	-	6
2. Организационно-правовая защита информации.					
	Государственная система защиты информации. Основные законодательные акты в области информационной безопасности. Меры ответственности за нарушения в области информационной безопасности. Основные регуляторы в области информационной безопасности. Основные нормативные и методических документы ФСТЭК и ФСБ в области обеспечения защиты конфиденциальной информации, в том числе персональных данных. Организационные методы защиты информации. Понятие политики информационной безопасности. Понятие объекта информатизации и его аттестации. Понятие лицензирования, стандартизации и сертификации в области информационной безопасности.	4	6	-	13
3. Уязвимости и угрозы информационной безопасности.					
	Уязвимости информационной безопасности. Угрозы информационной безопасности. Защита информации от несанкционированного доступа. Понятие риск-ориентированного подхода к обеспечению информационной безопасности. Понятие моделирования угроз информационной безопасности.	2	6	-	6
4. Техническая защита информации.					
	Понятие инженерно-технической защиты информации. Технические каналы утечки информации. Понятие и классификация визуально-оптических каналов утечки информации. Понятие и классификация каналов утечки акустической (речевой) информации. Понятие материально-вещественных каналов утечки информации. Понятие и классификация радиоэлектронных каналов утечки информации. Криптографические методы защиты информации. Системы шифрования. Понятие симметричной системы шифрования.	4	8	-	10

	Понятие асимметричной системы				
--	-------------------------------	--	--	--	--

	шифрования. Понятие электронной подписи.				
5. Защита информации в компьютерных сетях.					
	Понятие защиты информации в компьютерных сетях. Защита информации на компьютерах. Защита информации в локальных и глобальных сетях. Понятие системы защиты информации. Основные подсистемы обеспечения информационной безопасности. Программно-аппаратные средства обеспечения информационной безопасности.	4	10	-	11
	ВСЕГО	14	56	-	38

#### 4.2. Содержание лабораторных(семинарских) занятий

№ п/п	Наименование раздела дисциплины	Тема практического занятия	К-во часов	К-во часов СРС
семестр No 5				
1	Основные понятия информационной безопасности	Основные термины и определения в области информационной безопасности. Понятие комплексной защиты информации. Общий порядок работы с информацией ограниченного доступа.	4	4
2	Организационно-правовая защита информации	Основные законодательные акты в области информационной безопасности. Примеры нормативных и методических документов ФСТЭК и ФСБ в области обеспечения защиты конфиденциальной информации, в том числе персональных данных. Понятие аттестации объекта информатизации. Понятие лицензирования, стандартизации и сертификации в области информационной безопасности.	4	4
3	Уязвимости и угрозы информационной безопасности	Понятие защиты информации от несанкционированного доступа. Понятие риск-ориентированного информационного моделирования безопасности.  подхода к обеспечению безопасности. Понятие угроз информационной	6	6
4	Техническая защита	Понятие и классификация визуально-оптических каналов утечки информации. Понятие и	6	6

	информации	классификация каналов утечки акустической (речевой) информации. Понятие и классификация радиоэлектронных каналов утечки информации. Понятие симметричной системы шифрования. Понятие асимметричной системы шифрования. Понятие электронной подписи.		
5	Защита информации в компьютерных сетях	Понятие системы защиты информации. Основные принципы построения систем защиты информации.  Основные подсистемы информационной безопасности. функционирования систем вторжений. Механизмы безопасности в Windows и Linux. Наложённые программно-аппаратные средства обеспечения информационной безопасности. Защита локальных сетей с помощью межсетевых экранов.  обеспечения Принцип обнаружения	8	6
ИТОГО:			28	28
ВСЕГО:				56

#### **4.3. Содержание практических занятий**

Не предусмотрено учебным планом

#### **4.4. Содержание курсового проекта/работы**

Не предусмотрено учебным планом

#### **4.5. Содержание расчетно-графического задания, индивидуальных домашних заданий**

Индивидуальное домашнее задание имеет целью более углубленное изучение одного из направлений в рамках информационной безопасности. Оформляется в виде реферата. Перечень тем, для выполнения ИДЗ представлен ниже.

1. Порядок подготовки документов к открытой печати, с учетом требований к информации ограниченного доступа.

2. Электронная подпись. Технология ЭЦП.

3. Международные документы и стандарты в области информационной безопасности.

4. Методы борьбы с утечкой информации по визуально-оптическим каналам.

5. Методы борьбы с утечкой информации по акустическим (речевым) каналам.
6. Методы борьбы с утечкой информации по радиоэлектронным (электромагнитным) каналам.
7. Методы борьбы с утечкой информации по радиоэлектронным (электрическим) каналам.
8. Основные свойства информации. Важность, полнота, адекватность, релевантность
9. Физическая защита информационных систем.
10. Характеристика программно-аппаратных средств защиты информации (не рассматриваемых в курсе дисциплины).
11. Этапы создания систем защиты информации.
12. Защита информации. Основные принципы обеспечения информационной безопасности.
13. Информация. Виды информации, свойства и понятие информации в контексте информационной безопасности.
14. Антивирусы и антивирусная защита. Классификация вредоносных программ.
15. Межсетевые экраны и методы создания защищенных систем, включающих межсетевые экраны.
  16. Особенности защиты различных операционных систем.
  17. Аппаратные средства защиты информации.
  18. Протоколы PPP, SMTP, FTP и методы создания защищенного обмена
  19. Обеспечение безопасности при работе с электронной почтой.
  20. Резервирование информации. Средства создания резервных копий.
  21. Применение криптографических методов для защиты информации.
  22. Физическое разрушение информационных систем и методы защиты от  
физического воздействия.
  23. Троянские кони, люки и технология салями.
  24. Технология VPN. Построение защищенных каналов связи.



25. Сертификаты. Протокол HTTPS. Центры сертификации.
26. Социальная инженерия как способ мошенничества в киберпространстве.
27. Популярные способы мошенничества в киберпространстве.
28. Инструменты безопасности информации, реализованные в операционной системе Windows.
29. Инструменты безопасности информации, реализованные в операционной системе Linux.

## **6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ**

### **6.1. Материально-техническое обеспечение**

No	Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
1.	Учебная аудитория для проведения лекционных занятий	Специализированная мебель. Мультимедийная установка, экран, доски
2.	Учебная аудитория для проведения лабораторных занятий	Специализированная мебель. Компьютеры на базе процессоров Intel или AMD.
3.	Зал электронных ресурсов, здание библиотеки, No 302 Читальный зал учебной литературы, здание библиотеки, No 303	Специализированная мебель. Компьютерная техника, подключенная к сети интернет и имеющая доступ в электронно-образовательную среду

### **6.2. Лицензионное и свободно распространяемое программное обеспечение**

No	Перечень лицензионного программного обеспечения.	Реквизиты подтверждающего документа
1.	Microsoft Windows 10 Корпоративная	(Соглашение Microsoft Open Value Subscription V6328633 Соглашение действительно с 02.10.2017 по 23.10.2023). Договор поставки ПО 0326100004117000038-0003147-01 от 06.10.2017.
2.	Microsoft Office Professional Plus 2016	(Соглашение Microsoft Open Value Subscription V6328633 Соглашение действительно с 02.10.2017 по 23.10.2023). Договор поставки ПО 0326100004117000038-0003147-01

		от 06.10.2017.
3.	Google Chrome	Свободно распространяемое ПО согласно условиям лицензионного соглашения
4.	Среды программирования Free Pascal, Dev C++ или CodeBlocks	Свободно распространяемое ПО согласно условиям лицензионного соглашения

### **6.3. Перечень учебных изданий и учебно-методических материалов**

1. Информационная безопасность. Национальные стандарты Российской Федерации: учебное пособие для студентов, обучающихся по программам высшего образования / Ю. А. Родичев. - Москва [и др.]: Питер, 2019. - 304 с.
2. Информационная безопасность: учебное пособие / Я. С. Гродзенский. - Москва: Проспект, 2021. - 142 с.
3. Основы информационной безопасности: учебное пособие для студентов вузов, по направлению «Информационные системы и технологии» / Ю. Ю. Громов [и др.]. - Старый Оскол: ТНТ, 2017. - 382 с.
4. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— М.: ДМК Пресс, 2010.— 544 с.— Режим доступа: <http://www.iprbookshop.ru/7943>.— ЭБС «IPRbooks», по паролю
5. Горбенко А.О. Основы информационной безопасности (введение в профессию) [Электронный ресурс]: учебное пособие / А.О. Горбенко. — Электрон. текстовые данные. — СПб.: Интермедия, 2017. — 335 с. — 978-5-4383-0136-3. — Режим доступа: <http://www.iprbookshop.ru/66797.html>. — ЭБС «IPRbooks», по паролю
6. Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 с. — 978-5-94774-821-5. — Режим доступа: <http://www.iprbookshop.ru/52209.html>. — ЭБС «IPRbooks», по паролю

### **6.4. Перечень интернет ресурсов, профессиональных баз данных, информационно-справочных систем**

1. Электронная библиотека (на базе ЭБС «БиблиоТех») — Режим доступа: <http://ntb.bstu.ru>

2. Электронно-библиотечная система IPRbooks — Режим доступа:

<http://www.iprbookshop.ru>

3. Электронно-библиотечная система «Университетская библиотека ONLINE»

— Режим доступа: <http://www.biblioclub.ru/>

Рабочая программа дисциплины **«Основы и стандарты информационной безопасности»** составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.02 «Информационные системы и технологии», утвержденного приказом Министерства образования и науки Российской Федерации от «\_\_19\_\_» сентября 2017 г. № 926(ред.8.02.2021).

Программу составили:

Старший преподаватель кафедры «Информационные системы и технологии»  
Албагачиева М.Я.

Программа одобрена на заседании кафедры «Информационные системы и технологии»

Протокол № 6 от «03» марта 2025 года

Программа одобрена Учебно-методическим советом физико-математического факультета

Протокол №7 от «13» марта 2025 года

Приложение

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ (МОДУЛЯ)**

**Б1.В.11 Основы и стандарты информационной безопасности**

**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

# ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ НА РАЗЛИЧНЫХ ЭТАПАХ ИХ ФОРМИРОВАНИЯ, ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

**1. Компетенция ОПК-2.** Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности

Наименование индикатора достижения компетенции	Используемые средства оценивания
ОПК-2.1 Понимает принципы работы современных информационных технологий и программных средств, в том числе отечественного производства	устный опрос, зачет
ОПК-2.2 Использует современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности	собеседование, зачет

**2. Компетенция ОПК-3.** Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Наименование индикатора достижения компетенции	Используемые средства оценивания
ОПК-3.2 Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	устный опрос, зачет
ОПК-3.3 Подготавливает обзоры, аннотации, рефераты научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	собеседование, зачет

## Типовые контрольные задания для промежуточной аттестации

### Перечень контрольных вопросов (типовых заданий) для зачета

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
1.	Основные понятия информационной	В чем состоит актуальность проблем информационной безопасности?

	безопасности	<p>Дать определение понятию Информация.</p> <p>Дать определение понятию Информационная безопасность.</p> <p>Как классифицируется информация?</p> <p>Дать определение Защите информации.</p> <p>Перечислить аспекты информационной безопасности.</p> <p>Раскрыть аспект информационной безопасности – конфиденциальность.</p> <p>Раскрыть аспект информационной безопасности – целостность. Раскрыть аспект информационной безопасности – доступность. Что такое утечка, утечка информации?</p> <p>Дать определение защиты информации от несанкционированного доступа.</p>
2.	Организационно-правовая защита информации	<p>Что такое правовая защита информации?</p> <p>Что такое организационная защита информации?</p> <p>Раскрыть основное содержание ФЗ-149.</p> <p>Раскрыть основное содержание ФЗ-152.</p> <p>Раскрыть основное содержание ФЗ-63.</p> <p>Раскрыть основное содержание «Стратегии национальной безопасности РФ».</p> <p>Раскрыть основное содержание «Доктрины информационной безопасности РФ».</p> <p>Раскрыть назначение и структуру документа ФСТЭК – СТР-К. Понятие и общий порядок проведения аттестации объекта информатизации по требованиям информационной безопасности.</p> <p>Понятие и общий порядок проведения сертификации в области информационной безопасности.</p> <p>Дать понятие лицензированию деятельности в области защиты информации.</p> <p>Дать понятие стандартизации в области информационной безопасности.</p>
3.	Уязвимости и угрозы информационной безопасности	<p>Что такое уязвимость?</p> <p>Что такое угроза информации?</p> <p>Дать классификацию угроз по аспекту конфиденциальность, привести примеры.</p> <p>Дать классификацию угроз по аспекту целостность, привести примеры.</p> <p>Дать классификацию угроз по аспекту доступность, привести примеры.</p> <p>Дать классификацию угроз по происхождению и способу осуществления, привести примеры.</p> <p>Дать понятие актуальности угрозы.</p> <p>Дать понятие риск-ориентированному подходу при обеспечении информационной безопасности.</p>
		Основное содержание документа ФСТЭК «Методика оценки

		угроз безопасности информации».
4.	Техническая защита информации	<p>Дать определение техническому каналу утечки информации (ТКУИ).  Изобразить и пояснить структуру ТКУИ.  Дать классификацию ТКУИ.</p> <p>Охарактеризовать визуально-оптический ТКУИ.  Охарактеризовать акустический (речевой) ТКУИ.  Дать характеристику материально-вещественному ТКУИ.  Дать классификацию и охарактеризовать радиоэлектронный ТКУИ.  Дать понятие криптографии и стеганографии  Охарактеризовать криптографические методы преобразования информации.  Дать понятие шифрованию информации.  Охарактеризовать симметричную систему шифрования, ее достоинства и недостатки.  Охарактеризовать асимметричную систему шифрования, ее достоинства и недостатки.  Назначение и функции электронной подписи.  Пояснить принцип действия электронной подписи.</p>
5.	Защита информации в компьютерных сетях	<p>Перечислить основные угрозы в компьютерных сетях.  Каковы особенности защиты информации в локальных компьютерных сетях?  Каковы особенности защиты информации в глобальных компьютерных сетях?  Что такое система защиты информации?  Дать понятие подсистем обеспечения информационной безопасности.  Программные и программно-аппаратные средства обеспечения информационной безопасности. Их особенности.  Пояснить принцип работы средств обнаружения вторжений.  Виды межсетевых экранов, их назначение и принцип работы.</p>

### **Типовые контрольные задания (материалы) для текущего контроля в семестре**

**Текущий контроль** осуществляется в течение семестра в форме собеседования и устного опроса.

Собеседования и устные опросы направлены на проверку степени усвоения материала и понимания теоретических сведений, используемых в процессе выполнения работы. Примерные перечень вопросов для контроля знаний приведен в таблице:

Тематика дисциплины	Контрольные вопросы
---------------------	---------------------



Т. 1. Основные понятия информационной безопасности	<ol style="list-style-type: none"> <li>1. В чем состоит актуальность проблем информационной безопасности?</li> <li>2. Дать определение понятиям Информация, Информационная безопасность, Защита информации, Конфиденциальная информация.</li> <li>3. Каковы аспекты информационной безопасности?</li> <li>4. Что такое конфиденциальность, целостность, доступность?</li> <li>5. Как классифицируется информация?</li> <li>6. Утечка информации.</li> <li>7. Защита информации от несанкционированного доступа.</li> </ol>
Т.2. Организационно- правовая защита информации	<ol style="list-style-type: none"> <li>1. Основные положения Федерального закона «Об информации, информационных технологиях и защите информации».</li> <li>2. Основные положения Федерального закона «О персональных данных».</li> <li>3. Основные положения Федерального закона «Об электронной подписи».</li> <li>4. Виды информации ограниченного доступа.</li> <li>5. Основные положения «Стратегии национальной безопасности РФ».</li> <li>6. Основные положения «Доктрины информационной безопасности РФ».</li> <li>7. Структура документа ФСТЭК – СТР-К.</li> <li>8. Дать понятие аттестации объекта автоматизации.</li> <li>9. Дать понятие сертификации средств защиты информации.</li> <li>10. Дать понятие лицензированию деятельности в области защиты информации.</li> <li>11. Привести примеры стандартов в области информационной безопасности и их основное содержание.</li> </ol>
Т.3. Уязвимости и угрозы информационной безопасности	<ol style="list-style-type: none"> <li>1. Что такое уязвимость?</li> <li>2. Что такое угроза информации?</li> <li>3. Дать классификацию угроз по аспектам информационной безопасности, привести примеры.</li> <li>4. Дать классификацию угроз по происхождению и способу осуществления, привести примеры.</li> <li>5. Дать понятие угрозам конфиденциальности, доступности, целостности.</li> <li>6. Дать понятие риск-ориентированному подходу при обеспечении информационной безопасности.</li> <li>7. Основное содержание документа ФСТЭК «Методика оценки угроз безопасности информации».</li> </ol>
Т.4. Техническая защита	<ol style="list-style-type: none"> <li>1. Понятие и структура технического канала утечки информации.</li> </ol>

информации	<p>2. Дать классификацию техническим каналам утечки информации. 3. Пояснить сущность и классифицировать визуально-оптический, акустический (речевой), радиоэлектронный, материально-вещественный каналы утечки информации.</p> <p>4. Какие криптографические методы обработки информации используются в области информационной безопасности?</p> <p>5. Что такое симметричная система шифрование, ее достоинства и недостатки?</p> <p>6. Что такое асимметричная система шифрование, ее достоинства и недостатки?</p> <p>7. Дать понятие электронной подписи.</p>
Т.5. Защита информации в компьютерных сетях	<p>1. Пояснить понятия: Информационная система и Система защиты информации.</p> <p>2. Какие известны основные принципы построения систем защиты информации?</p> <p>3. Какие известны подсистемы обеспечения информационной безопасности?</p> <p>4. Дать понятие программно-аппаратным средствам обеспечения информационной безопасности, привести примеры.</p> <p>5. Дать понятие средства обнаружения вторжений.</p> <p>6. Классификация, назначение и принцип работы межсетевых экранов.</p>

## Описание критериев оценивания компетенций и шкалы оценивания

При промежуточной аттестации в форме зачета используется следующая шкала оценивания: зачтено, не зачтено.

Критериями оценивания достижений показателей являются:

Оценка преподавателем выставляется интегрально с учётом всех показателей и критериев оценивания. оценка сформированности компетенций по показателю Знания.

Наименование показателя оценивания результата обучения по дисциплине	Критерий оценивания
Знания	Знание принципов работы технологий, реализованных в программных средствах обеспечения защиты информации: идентификации и аутентификации, регистрации и учета,

	криптографической защиты, контроля целостности		
	Знание возможностей современных программных и программно-аппаратных средств защиты информации, в том числе отечественного производства: «Аккорд», Secret net и Dallas lock		
	Знание содержания основных Федеральных законов РФ, постановлений правительства РФ и указов Президента РФ в области информационной безопасности; меры ответственности за нарушения в области информационной безопасности		
	Знание основных требований законодательства и регуляторов к подготовке обзоров, аннотаций, рефератов научных докладов, публикаций и библиографий по научно-исследовательской работе, содержащих сведения ограниченного доступа		
	Объем освоенного материала		
	Полнота ответов на вопросы		
	Четкость изложения и интерпретации знаний		
Умения	Умение осуществить выбор программно-аппаратного средства защиты информации для нейтрализации угрозы		
	несанкционированного доступа		
	Умение анализировать основные положения законодательства в области безопасности информации		
	Умение использовать руководящие документы регуляторов в области информационной безопасности		
Навыки	Владение навыками использования нормативных правовых актов, основных нормативных и методических документов ФСТЭК и Роскомнадзора в области обеспечения защиты конфиденциальной информации, в том числе персональных данных		
	Владение навыками оформления обзоров, аннотаций, рефератов научных докладов, публикаций и библиографии по научно-исследовательской работе в соответствии с требованиями законодательства и регуляторов		

Критерий	Уровень освоения и оценка			
	незачтено	незачтено	зачтено	зачтено

Знание принципов работы технологий, реализованных в программных средствах обеспечения защиты информации: идентификации и аутентификации, регистрации и учета, криптографической защиты, контроля целостности	Не знает принципы работы технологий, реализованных в программных средствах обеспечения защиты информации: идентификации и аутентификации, регистрации и учета, криптографической защиты, контроля целостности	Знает принципы работы некоторых технологий, реализованных в программных средствах обеспечения защиты информации: идентификации и аутентификации, регистрации и учета, криптографической защиты, контроля целостности	Знает принципы работы технологий, реализованных в программных средствах обеспечения защиты информации: идентификации и аутентификации, регистрации и учета, криптографической защиты, контроля целостности	Знает и понимает принципы работы технологий, реализованных в программных средствах обеспечения защиты информации: идентификации и аутентификации, регистрации и учета, криптографической защиты, контроля целостности
Знание возможностей современных программных и программно-аппаратных средств защиты информации, в том числе отечественного производства: «Аккорд», Secret net и Dallas lock	Не знает возможности современных программных и программно-аппаратных средств защиты информации, в том числе отечественного производства: «Аккорд», Secret net и Dallas lock	Знает некоторые возможности современных программных и программно-аппаратных средств защиты информации, в том числе отечественного производства: «Аккорд», Secret net и Dallas lock	Знает возможности современных программных и программно-аппаратных средств защиты информации, в том числе отечественного производства: «Аккорд», Secret net и Dallas lock	Знает и понимает возможности современных программных и программно-аппаратных средств защиты информации, в том числе отечественного производства: «Аккорд», Secret net и Dallas lock
Знание содержания основных Федеральных законов РФ, постановлений	Не знает содержание основных Федеральных законов РФ, постановлений	Знает содержание некоторых Федеральных законов РФ, постановлений правительства РФ	Знает содержание Федеральных законов РФ, постановлений правительства	Знает содержание Федеральных законов РФ, постановлений правительства РФ и указов Президента
правительства РФ и указов Президента РФ в области информационной безопасности; меры ответственности за нарушения в области информационной безопасности	правительства РФ и указов Президента РФ в области информационной безопасности; меры ответственности за нарушения в области информационной безопасности	и указов Президента РФ в области информационной безопасности; меры ответственности за нарушения в области информационной безопасности	РФ и указов Президента РФ в области информационной безопасности; меры ответственности за нарушения в области информационной безопасности	РФ в области информационной безопасности; меры ответственности за нарушения в области информационной безопасности в полном объеме
Знание основных требований законодательства и	Не знает требований законодательства и	Знает некоторые требования законодательства и	Знает основные требования законодательства и	Знает основные требования законодательства и

регуляторов к подготовке обзоров, аннотаций, рефератов научных докладов, публикаций и библиографий по научно-исследовательской работе, содержащих сведения ограниченного доступа	регуляторов к подготовке обзоров, аннотаций, рефератов научных докладов, публикаций и библиографий по научно-исследовательской работе, содержащих сведения ограниченного доступа	регуляторов к подготовке обзоров, аннотаций, рефератов научных докладов, публикаций и библиографий по научно-исследовательской работе, содержащих сведения ограниченного доступа	регуляторов к подготовке обзоров, аннотаций, рефератов научных докладов, публикаций и библиографий по научно-исследовательской работе, содержащих сведения ограниченного доступа	регуляторов к подготовке обзоров, аннотаций, рефератов научных докладов, публикаций и библиографий по научно-исследовательской работе, содержащих сведения ограниченного объема
Объем освоенного материала	Не знает значительной части материала дисциплины	Знает только основной материал дисциплины, не усвоил его деталей	Знает материал дисциплины в достаточном объеме	Обладает твердым и полным знанием материала дисциплины, владеет дополнительными знаниями
Полнота ответов на вопросы	Не дает ответы на большинство вопросов	Дает неполные ответы на все вопросы	Дает ответы на вопросы, но не все - полные	Дает полные, развернутые ответы на поставленные вопросы
Четкость изложения и интерпретации знаний	Излагает знания без логической последовательности	Излагает знания с нарушениями в логической последовательности	Излагает знания без нарушений в логической последовательности	Излагает знания в логической последовательности, самостоятельно их интерпретируя и анализируя
	Не иллюстрирует изложение поясняющими схемами, рисунками и примерами	Выполняет поясняющие схемы и рисунки небрежно и с ошибками	Выполняет поясняющие рисунки и схемы корректно и понятно	Выполняет поясняющие рисунки и схемы точно и аккуратно, раскрывая полноту усвоенных знаний
	Неверно излагает и интерпретирует знания	Допускает неточности в изложении и интерпретации знаний	Грамотно и по существу излагает знания	Грамотно и точно излагает знания, делает самостоятельные выводы

Оценка сформированности компетенций по показателю Умения.

Критерий	Уровень освоения и оценка
----------	---------------------------

	незачтено	незачтено	зачтено	зачтено
Умение осуществить выбор программно-аппаратного средства защиты информации для нейтрализации угрозы несанкционированного доступа	Не умеет выбирать программно-аппаратные средства защиты информации для нейтрализации угрозы несанкционированного доступа	Выбирает программно-аппаратные средства защиты информации для нейтрализации угрозы несанкционированного доступа не обоснованно	Выбирает программно-аппаратные средства защиты информации для нейтрализации угрозы несанкционированного доступа не достаточно рационально	Рационально и обоснованно выбирает программно-аппаратные средства защиты информации для нейтрализации угрозы несанкционированного доступа
Умение анализировать основные положения законодательства в области безопасности информации	Не умеет анализировать основные положения законодательства в области безопасности информации	Допускает неточности в анализе основных положений законодательства в области безопасности информации	Умеет анализировать основные положения законодательства в области безопасности информации	Умеет анализировать основные положения законодательства в области безопасности информации и делать обобщающие выводы
Умение использовать руководящие документы регуляторов в области информационной безопасности	Не умеет использовать руководящие документы регуляторов в области информационной безопасности	Использование руководящих документов регуляторов в области информационной безопасности вызывает затруднения	Умеет использовать руководящие документы регуляторов в области информационной безопасности	Умело использует руководящие документы регуляторов в области информационной безопасности

Оценка сформированности компетенций по показателю Навыки.

Критерий	Уровень освоения и оценка			
	незачтено	незачтено	зачтено	зачтено
Владение навыками использования нормативных правовых актов, основных нормативных и	Не владеет навыками использования нормативных правовых актов, основных нормативных и	Не достаточно хорошо владеет навыками использования нормативных правовых актов, основных	Владеет навыками теоретического использования нормативных правовых актов, основных нормативных и	Профессионально владеет навыками использования нормативных правовых актов, основных нормативных и

методических документов ФСТЭК и Роскомнадзора в области	методических документов ФСТЭК и Роскомнадзора в области обеспечения	нормативных и методических документов ФСТЭК и	методических документов ФСТЭК и	методических документов ФСТЭК и Роскомнадзора в области обеспечения
обеспечения защиты конфиденциальной информации, в том числе персональных данных	защиты конфиденциальной информации, в том числе персональных данных	Роскомнадзора в области обеспечения защиты конфиденциальной информации, в том числе персональных данных	Роскомнадзор а в области обеспечения защиты конфиденциальной информации, в том числе персональных данных	защиты конфиденциальной информации, в том числе персональных данных
Владение навыками оформления обзоров, аннотаций, рефератов научных докладов, публикаций и библиографии по научно-исследовательской работе в соответствии с требованиями законодательства и регуляторов	Не владеет навыками оформления обзоров, аннотаций, рефератов научных докладов, публикаций и библиографии по научно-исследовательской работе в соответствии с требованиями законодательства и регуляторов	Не достаточно хорошо владеет навыками оформления обзоров, аннотаций, рефератов научных докладов, публикаций и библиографии по научно-исследовательской работе в соответствии с требованиями законодательства и регуляторов	Владеет навыками оформления обзоров, аннотаций, рефератов научных докладов, публикаций и библиографии по научно-исследовательской работе в соответствии с требованиями законодательства и регуляторов	Профессионально владеет навыками оформления обзоров, аннотаций, рефератов научных докладов, публикаций и библиографии по научно-исследовательской работе в соответствии с требованиями законодательства и регуляторов