ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.Б.13 Основы информационной безопасности

(код и наименование дисциплины согласно РУП)

Направление подготовки (специальность) 09.03.01 Информатика и вычислительная техника

Профиль подготовки (специализация) "Автоматизированные системы обработки информации и управления"

Квалификация (степень) выпускника бакалавр

(бакалавр, магистр, специалист)

Форма обучения заочная

(очная, заочная)

1. Цели освоения дисциплины

Целями освоения дисциплины «Основы информационной безопасности» являются:

- изучение современных методов обработки, преобразования и защиты информации в современных компьютерных системах;
- овладение основами криптологии, основными принципами, методами и алгоритмами эксплуатации программных систем сбора, закрытия, восстановления и аутентификации информации;
- изучение современных способов борьбы с несанкционированным блокированием, доступом, копированием, изменением и сбором информации.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Основы информационной безопасности» относится к базовой части. Требования к предшествующим знаниям представлены в таблице 2.1. Перечень дисциплин, для которых дисциплина «Основы информационной безопасности» является основополагающей, представлен в табл. 2.2.

Таблица 2.1 – Требования к пререквизитам дисциплины

Дисциплина	Раздел
Алгебра и геометрия	Все разделы

Таблица 2.2 –Требования к постреквизитам дисциплины

Дисциплина	Раздел
Основы информационной безопасности	Программные средства защиты информации в телекоммуникационных сетях

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Таблица 3.1 – Взаимосвязь планируемых результатов обучения по дисциплине и планируемых результатов освоения образовательной программы

Индекс и содержание компетенции	Знания	Умения	Навыки и (или) опыт деятельности
ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности	Этап 1: основные стандарты в области инфокоммуникационных систем и технологий, в том числе стандарты Единой системы программной документации; Этап 2: методы и средства обеспечения информационной безопасности компьютерных систем.	Этап 1: инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем; Этап 2: инсталлировать, тестировать, испытывать и использовать программно-аппаратные	Этап 1: методами выбора элементной базы для построения различных архитектур вычислительных средств; Этап 2: методами защиты информации и конфигурирования комплексных систем защиты.

		средства вычислительных и информационных систем;	
ОПК-5 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Этап 1: основные стандарты в области инфокоммуникационных систем и технологий, в том числе стандарты Единой системы программной документации; Этап 2: методы и средства обеспечения информационной безопасности компьютерных систем.	Этап 1: инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем; Этап 2: инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем;	Этап 1: методами выбора элементной базы для построения различных архитектур вычислительных средств; Этап 2: методами защиты информации и конфигурирования комплексных систем защиты.

4. Объем дисциплины

Объем дисциплины «Основы информационной безопасности» составляет 6 зачетных единиц (216 академических часов), распределение объема дисциплины на контактную работу обучающихся с преподавателем (КР) и на самостоятельную работу обучающихся (СР) по видам учебных занятий и по периодам обучения представлено в таблице 4.1.

Таблица 4.1 –Распределение объема дисциплины
по видам учебных занятий и по периодам обучения, академические часы

№ п/п	Вид учебных занятий	Итого КР	Итого СР	Семестр №5		Семестр №6	
				КР	СР	КР	СР
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	Лекции (Л)	8		6		2	
2	Лабораторные работы (ЛР)						
3	Практические занятия (ПЗ)	8		4		4	
4	Семинары(С)						
5	Курсовое проектирование (КП)						
6	Рефераты (Р)						
7	Эссе (Э)						
8	Индивидуальные домашние задания (ИДЗ)						
9	Самостоятельное изучение вопросов (СИВ)		196		98		98
10	Подготовка к занятиям (ПкЗ)						
11	Промежуточная аттестация	4				4	
12	Наименование вида промежуточной аттестации					Экзамен	
13	Всего	20	196	10	98	6	98

5. Структура и содержание дисциплины

Структура дисциплины представлена в таблице 5.1.

Таблица 5.1 – Структура дисциплины

№ п/п	Наименования разделов и тем	Семестр	Объем работы по видам учебных занятий, академические часы										Коды формируемых компетенций
			лекции	лабораторная работа	практические занятия	семинары	курсовое проектирование	рефераты (эссе)	индивидуальные домашние задания	самостоятельное изучение вопросов	подготовка к занятиям	промежуточная аттестация	
1	2	3	4	5	6	7	8	9	10	11	12	13	14
1.	**Раздел 1** **Введение. Основы криптологии.**	5	6		4					98			ОК-4 ОПК-5
1.1.	**Тема 1** Проблема ЗИ. Место ЗИ в системе национальной безопасности. Системный анализ как составная часть безопасности. Риск. Группы риска. Пути несанкционированного получения информации. Цель и необходимость закрытия информации. Объекты защиты, направления, методы и средства ЗИ. Комплексность и системность ЗИ. Законодательный, административный, процедурный и программно-технический уровни обеспечения безопасности. Основные понятия и	5	3		2					49			ОК-4 ОПК-5

№ п/п	Наименования разделов и тем	Семестр	Объем работы по видам учебных занятий, академические часы										Коды формируемых компетенций
			лекции	лабораторная работа	практические занятия	семинары	курсовое проектирование	рефераты (эссе)	индивидуальные домашние задания	самостоятельное изучение вопросов	подготовка к занятиям	промежуточная аттестация	
1	2	3	4	5	6	7	8	9	10	11	12	13	14
	определения теории ЗИ. Становление и развитие теории и техники ЗИ.												
1.2.	**Тема 2** Классификация методов ЗИ. Классификация по виду ЗИ, способу ЗИ, разновидности преобразования информации, способу реализации. Криптология, криптография и криптоанализ. Основные понятия криптологии. Стойкость, защищенность, имитостойкость, аутентичность.	5	3		2					49			ОК-4 ОПК-5
2.	**Контактная работа**	5	6		4								
3.	**Самостоятельная работа**	5								98			
4.	**Объем дисциплины в семестре**	5	6		4					98			
5.	**Раздел 2 Современные криптографические методы. Развитие и совершенствование криптографического закрытия информации**	6	2		4					98			ОК-4 ОПК-5
5.1.	**Тема 3** Криптография как наука. Понятие криптографического ключа. История криптографии	6	1		2					49			ОК-4 ОПК-5

№ п/п	Наименования разделов и тем	Семестр	Объем работы по видам учебных занятий, академические часы										Коды формируемых компетенций
			лекции	лабораторная работа	практические занятия	семинары	курсовое проектирование	рефераты (эссе)	индивидуальные домашние задания	самостоятельное изучение вопросов	подготовка к занятиям	промежуточная аттестация	
1	2	3	4	5	6	7	8	9	10	11	12	13	14
	и классические способы шифрования: замена, подстановка, перестановка, аналитическое преобразование, использование таблиц Вижинера, шифр Вернама, гаммирование, использование алгебры матриц. Комбинированное шифрование. Другие виды шифрования: рассечение-разнесение, сжатие-расширение. Современные системы шифрования. Основные принципы построения криптоалгоритмов.												
5.2.	**Тема 4** Методы исследования криптографических алгоритмов. Классические методы ЗИ и стойкость шифрования. Основные методы дешифрования. Шифры Цезаря, Виженера. Раскрытие несовершенны шифров. Криптографическая модель Шеннона. Теория криптоанализа. Стойкость	6	1		2					49			ОК-4 ОПК-5

№ п/п	Наименования разделов и тем	Семестр	Объем работы по видам учебных занятий, академические часы										Коды формируемых компетенций
			лекции	лабораторная работа	практические занятия	семинары	курсовое проектирование	рефераты (эссе)	индивидуальные домашние задания	самостоятельное изучение вопросов	подготовка к занятиям	промежуточная аттестация	
1	2	3	4	5	6	7	8	9	10	11	12	13	14
	шифра. Способы кодирования: смысловое, символьное.												
6.	**Контактная работа**	6	2		4							4	
7.	**Самостоятельная работа**	6								98			
8.	**Объем дисциплины в семестре**	6	2		4					98		4	
10.	**Всего по дисциплине**		8		8					196		4	

5.2. Содержание дисциплины

5.2.1 – Темы лекций

№ п.п.	Наименование темы лекции	Объем, академические часы
Л-1	Проблема ЗИ. Место ЗИ в системе национальной безопасности. Системный анализ как составная часть безопасности. Риск. Группы риска. Пути несанкционированного получения информации. Цель и необходимость закрытия информации. Объекты защиты, направления, методы и средства ЗИ. Комплексность и системность ЗИ. Законодательный, административный, процедурный и программно-технический уровни обеспечения безопасности. Основные понятия и определения теории ЗИ. Становление и развитие теории и техники ЗИ.	3
Л-2	Классификация методов ЗИ. Классификация по виду ЗИ, способу ЗИ, разновидности преобразования информации, способу реализации. Криптология, криптография и криптоанализ. Основные понятия криптологии. Стойкость, защищенность, имитостойкость, аутентичность.	3
Л-3	Криптография как наука. Понятие криптографического ключа. История криптографии и классические способы шифрования: замена, подстановка, перестановка, аналитическое преобразование, использование таблиц Вижинера, шифр Вернама, гаммирование, использование алгебры матриц. Комбинированное шифрование. Другие виды шифрования: рассечение-разнесение, сжатие-расширение. Современные системы шифрования. Основные принципы построения криптоалгоритмов.	1
Л-4	Методы исследования криптографически алгоритмов. Классические методы ЗИ и стойкость шифрования. Основные методы дешифрования. Шифры Цезаря, Виженера. Раскрытие несовершенны шифров. Криптографическая модель Шеннона. Теория криптоанализа. Стойкость шифра. Способы кодирования: смысловое, символьное.	1
Итого по дисциплине		8

5.2.2 – Темы лабораторных работ (не предусмотрены учебным планом)

5.2.3 –Темы практически занятий

№ п.п.	Наименование темы занятия	Объем, академические часы
ПЗ-1	Проблема ЗИ. Место ЗИ в системе национальной безопасности. Системный анализ как составная часть безопасности. Риск. Группы риска. Пути несанкционированного получения информации. Цель и необходимость закрытия информации. Объекты защиты, направления, методы и средства ЗИ. Комплексность и системность ЗИ. Законодательный, административный, процедурный и программно-технический уровни обеспечения безопасности. Основные понятия и определения теории ЗИ. Становление и развитие теории и техники ЗИ.	2
ПЗ-2	Классификация методов ЗИ. Классификация по виду ЗИ, способу ЗИ, разновидности преобразования информации, способу реализации. Криптология, криптография и	2

	криптоанализ. Основные понятия криптологии. Стойкость, защищенность, имитостойкость, аутентичность.	
ПЗ-3	Криптография как наука. Понятие криптографического ключа. История криптографии и классические способы шифрования: замена, подстановка, перестановка, аналитическое преобразование, использование таблиц Вижинера, шифр Вернама, гаммирование, использование алгебры матриц. Комбинированное шифрование. Другие виды шифрования: рассечение-разнесение, сжатие-расширение. Современные системы шифрования. Основные принципы построения криптоалгоритмов.	2
ПЗ-4	Методы исследования криптографически алгоритмов. Классические методы ЗИ и стойкость шифрования. Основные методы дешифрования. Шифры Цезаря, Виженера. Раскрытие несовершенны шифров. Криптографическая модель Шеннона. Теория криптоанализа. Стойкость шифра. Способы кодирования: смысловое, символьное.	2
Итого по дисциплине		8

5.2.4 – Темы семинарски занятий (не предусмотрены учебным планом)

5.2.5 Темы курсовых работ (проектов) (не предусмотрены учебным планом)

5.2.6 Темы рефератов (не предусмотрены)

5.2.7 Темы эссе (не предусмотрены)

5.2.8 Темы индивидуальны домашних заданий (не предусмотрены)

5.2.9 – Вопросы для самостоятельного изучения

№ п.п.	Наименования темы	Наименование вопроса	Объем, академические часы
1.	Проблема ЗИ. Место ЗИ в системе национальной безопасности. Системный анализ как составная часть безопасности. Риск. Группы риска. Пути несанкционированного получения информации. Цель и необходимость закрытия информации. Законодательный, административный, процедурный и программно-технический уровни обеспечения безопасности. Основные понятия и определения теории ЗИ. Становление и развитие теории и те никих ЗИ.	Законодательные и правовые основы защиты компьютерной информации и информационных технологий	49
2.	Классификация методов ЗИ. Классификация по виду ЗИ, способу ЗИ, разновидности	Криптология, криптография и криптоанализ.	49

	преобразования информации, способу реализации. Криптология, криптография и криптоанализ. Основные понятия криптологии. Стойкость, защищенность, имитостойкость, аутентичность.		
3.	Криптография как наука. Понятие криптографического ключа. История криптографии и классические способы шифрования: замена, подстановка, перестановка, аналитическое преобразование, использование таблиц Вижинера, шифр Вернама, гаммирование, использование алгебры матриц. Комбинированное шифрование. Другие виды шифрования: рассечение-разнесение, сжатие-расширение. Современные системы шифрования. Основные принципы построения криптоалгоритмов.	В чем заключаются традиционные методы шифрования, являющиеся базовыми для современны производны шифров с секретным ключом. В чем заключается правило Кирхгоффа. Какой шифр считается стойким. В чем заключаются принципы блочного шифрования. В чем заключаются принципы поточного шифрования.	49
4.	Методы исследования криптографических алгоритмов. Классические методы ЗИ и стойкость шифрования. Основные методы дешифрования. Шифры Цезаря, Виженера. Раскрытие несовершенны шифров. Криптографическая модель Шеннона. Теория криптоанализа. Стойкость шифра. Способы кодирования: смысловое, символьное.	Основные преимущества и недостатки симметричны и асимметричны криптосистем. Как строится (реализуется) гибридная криптосистема. В чем ее преимущество по сравнению с другими типами криптосистем Какие шифры называются комбинированными (производными) и какие базовые методы шифрования используются при и реализации	49
Итого по дисциплине			196

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература, необходимая для освоения дисциплины

1.Технологии и продукты Microsoft в обеспечении информационной безопасности. - Авдошин С.М., Сердюк В.А., Савельева А.А.ИНТУИТ • 2010 год • 455 страниц (книгафонд)

6.2 Дополнительная литература, необходимая для освоения дисциплины

1. Основы информационной безопасности при работе на компьютере. - Фаронов А.Е. ИНТУИТ • 2011 год • 157 страниц (КНИГАФОНД).

2. Обеспечение безопасности персональных данных Скрипник Д.А. ИНТУИТ • 2011 год • 122 страницы (КНИГАФОНД).

6.3 Методические указания для обучающихся по освоению дисциплины и другие материалы к занятиям

Электронное учебное пособие включающее:

- конспект лекций;
- методические указания по выполнению практически (семинарских) работ.

6.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Электронное учебное пособие включающее:

- методические рекомендации по самостоятельному изучению вопросов

6.5 Перечень информационных технологий, используемы при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

1. Microsoft Office

6.6 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимы для освоения дисциплины

1. http://www.knigafund.ru/ - ЭБС

7. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Занятия лекционного типа проводятся в аудитории, оборудованной мультимедиа проектором, компьютером, учебной доской.

Таблица 7.1 – Материально-техническое обеспечение практических занятий

№ п.п.	Наименование темы	Название специализированной лаборатории	Название спецоборудования	Название технических и электронных средств обучения и контроля знаний
ПЗ-1	Проблема ЗИ. Место ЗИ в системе национальной безопасности. Системный анализ как составная часть безопасности. Риск. Группы риска. Пути несанкционированного получения информации. Цель и необходимость закрытия информации. Объекты защиты, направления, методы и средства ЗИ. Комплексность и системность ЗИ. Законодательный, административный, процедурный и программно-технический уровни обеспечения безопасности. Основные понятия и определения теории ЗИ. Становление и развитие теории и техники ЗИ.	941 лаборатория программно-аппаратных средств защиты информации, 943 лаборатория технологий,	ПЭВМ (по количеству обучающихся)	Microsoft Office

		методов программирования и программного обеспечения		
ПЗ-2	Классификация методов ЗИ. Классификация по виду ЗИ, способу ЗИ, разновидности преобразования информации, способу реализации. Криптология, криптография и криптоанализ. Основные понятия криптологии. Стойкость, защищенность, имитостойкость, аутентичность.	941 лаборатория программно-аппаратных средств защиты информации, 943 лаборатория технологий, методов программирования и программного обеспечения	ПЭВМ (по количеству обучающихся)	Microsoft Office
ПЗ-3	Криптография как наука. Понятие криптографического ключа. История криптографии и классические способы шифрования: замена, подстановка, перестановка, аналитическое преобразование, использование таблиц Вижинера, шифр Вернама, гаммирование, использование алгебры матриц. Комбинированное шифрование. Другие виды шифрования: рассечение-разнесение, сжатие-расширение. Современные системы шифрования. Основные принципы построения криптоалгоритмов.	941 лаборатория программно-аппаратных средств защиты информации, 943 лаборатория технологий, методов программирования и программного обеспечения	ПЭВМ (по количеству обучающихся)	Microsoft Office
ПЗ-4	Методы исследования криптографически алгоритмов. Классические методы ЗИ и стойкость шифрования. Основные методы дешифрования. Шифры Цезаря, Виженера. Раскрытие несовершенны шифров. Криптографическая модель Шеннона.	941 лаборатория программно-	ПЭВМ (по количеству обучающихся)	Microsoft Office

	Теория криптоанализа. Стойкость шифра. Способы кодирования: смысловое, символьное.	аппаратных средств защиты информации, 943 лаборатория технологий, методов программирования и программного обеспечения		

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине представлен в Приложении 1.

Программа разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 09.03.01 Информатика и вычислительная техника, утвержденным приказом Министерства образования и науки РФ от 12 января 2016 г. № 5.

Разработал(и): _____ И.В. Засидкевич

МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

Приложение

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

Б1.Б.13 Основы информационной безопасности

Направление подготовки (специальность)
09.03.01 Информатика и вычислительная техника

Профиль подготовки (специализация)
“Автоматизированные системы обработки информации и управления**”**

Квалификация (степень) выпускника бакалавр

Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

Наименование и содержание компетенции
ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности

Знать:
Этап 1: основные стандарты в области инфокоммуникационных систем и технологий, в том числе стандарты Единой системы программной документации;
Этап 2: методы и средства обеспечения информационной безопасности компьютерных систем.
Уметь:
Этап 1: инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем;
Этап 2: инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем;
Владеть:
Этап 1: методами выбора элементной базы для построения различных архитектур вычислительных средств;
Этап 2: методами защиты информации и конфигурирования комплексных систем защиты.

ОПК-5 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Знать:
Этап 1: основные стандарты в области инфокоммуникационных систем и технологий, в том числе стандарты Единой системы программной документации;
Этап 2: методы и средства обеспечения информационной безопасности компьютерных систем.
Уметь:
Этап 1: инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем;
Этап 2: инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем;
Владеть:
Этап 1: методами выбора элементной базы для построения различных архитектур вычислительных средств;
Этап 2: методами защиты информации и конфигурирования комплексных систем защиты.

1. Показатели и критерии оценивания компетенций на различных этапах их формирования.

Таблица 1 - Показатели и критерии оценивания компетенций на 1 этапе

Наименование компетенции	**Критерии сформированности компетенции**	**Показатели**	**Способы оценки**
1	2	3	4
ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности	владеет способностью использовать основы правовых знаний в различных сферах деятельности	**Знать:** основные стандарты в области инфокоммуникационных систем и технологий, в том числе стандарты Единой системы программной документации; **Уметь:** инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем; **Владеть:** методами выбора элементной базы для построения различных архитектур вычислительных средств;	индивидуальный устный опрос, тестирование.
ОПК-5 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	владеет способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знать:** основные стандарты в области инфокоммуникационных систем и технологий, в том числе стандарты Единой системы программной документации; **Уметь:** инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем; **Владеть:** методами выбора элементной базы для построения различных архитектур вычислительных средств;	индивидуальный устный опрос, тестирование.

Таблица 2 - Показатели и критерии оценивания компетенций на 2 этапе

Наименование компетенции	**Критерии сформированности компетенции**	**Показатели**	**Способы оценки**
1	2	3	4
ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности	владеет способностью использовать основы правовых знаний в различных сферах деятельности	**Знать:** методы и средства обеспечения информационной безопасности компьютерных систем. **Уметь:** инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем; **Владеть:** методами защиты информации и конфигурирования комплексных систем защиты.	индивидуальный устный опрос, тестирование.
ОПК-5 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	владеет способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знать:** методы и средства обеспечения информационной безопасности компьютерных систем. **Уметь:** инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем; **Владеть:** методами защиты информации и конфигурирования комплексных систем защиты.	

2. Шкала оценивания.

Университет использует систему оценок соответствующего государственным регламентам в сфере образования и позволяющую обеспечивать интеграцию в международное образовательное пространство. Система оценок и описание систем оценок представлены в таблицах 3 и 4.

Таблица 3 - Система оценок

Диапазон оценки, в баллах	**Экзамен**		**Зачет**
	европейская шкала (ECTS)	традиционная шкала	
[95;100]	**A** – (5+)	отлично – (5)	зачтено
[85;95)	**B** – (5)		
[70,85)	**C** – (4)	хорошо – (4)	
[60;70)	**D** – (3+)	удовлетворительно – (3)	
[50;60)	**E** – (3)		незачтено
[33,3;50)	**FX** – (2+)	неудовлетворительно – (2)	
[0;33,3)	**F** – (2)		

Таблица 4 - Описание системы оценок

ECTS	**Описание оценок**	**Традиционная шкала**
A	**Превосходно** – теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному.	**отлично (зачтено)**
B	**Отлично** – теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом в основном сформированы, все предусмотренные программой обучения учебные задания выполнены, качество выполнения большинства из них оценено числом баллов, близким к максимальному.	

C	**Хорошо** – теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено максимальным числом баллов, некоторые виды заданий выполнены с ошибками.	**хорошо (зачтено)**
D	**Удовлетворительно** – теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, возможно, содержат ошибки.	**удовлетворительно (зачтено)**
E	**Посредственно** – теоретическое содержание курса освоено частично, некоторые практические навыки работы не сформированы, многие предусмотренные программой обучения учебные задания не выполнены, либо качество выполнения некоторых из них оценено числом баллов, близким к минимальному	**удовлетворительно (незачтено)**
FX	**Условно неудовлетворительно** – теоретическое содержание курса освоено частично, необходимые практические навыки работы не сформированы, большинство предусмотренных программой обучения учебных заданий не выполнено, либо качество их выполнения оценено числом баллов, близким к минимальному; при дополнительной самостоятельной работе над материалом курса возможно повышение качества выполнения учебных заданий.	**неудовлетворительно (незачтено)**
F	**Безусловно неудовлетворительно** – теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, все выполненные учебные задания содержат грубые ошибки, дополнительная самостоятельная работа над материалом курса не приведет к какому-либо значимому повышению качества выполнения учебных заданий.	

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности,

характеризующих этапы формирования компетенций в процессе освоения образовательной программы.

Таблица 5 - ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности. Этап 1

Наименование знаний, умений, навыков и (или) опыта деятельности	Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности
Знать: основные стандарты в области инфокоммуникационных систем и технологий, в том числе стандарты Единой системы программной документации;	1. Кто является основным ответственным за определение уровня классификации информации? а) Руководитель среднего звена б) Высшее руководство +в) Владелец г) Пользователь 2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности? +а) Сотрудники б) Хакеры в) Атакующие г) Контрагенты (лица, работающие по договору) 3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству? а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации +в) Улучшить контроль за безопасностью этой информации г) Снизить уровень классификации этой информации 4. Что самое главное должно продумать руководство при классификации данных? +а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным б) Необходимый уровень доступности, целостности и конфиденциальности в) Оценить уровень риска и отменить контрмеры г) Управление доступом, которое должно защищать данные 5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены? а) Владельцы данных б) Пользователи в) Администраторы +г) Руководство
Уметь:	6. Что такое процедура?

инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем;	А) Правила использования программного и аппаратного обеспечения в компании +Б) Пошаговая инструкция по выполнению задачи С) Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах Г) Обязательные действия 7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании? +А) Поддержка высшего руководства Б) Эффективные защитные меры и методы их внедрения С) Актуальные и адекватные политики и процедуры безопасности Г) Проведение тренингов по безопасности для всех сотрудников 8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков? А) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски Б) Когда риски не могут быть приняты во внимание по политическим соображениям С) Когда необходимые защитные меры слишком сложны +Г) Когда стоимость контрмер превышает ценность актива и потенциальные потери 9. Что такое политики безопасности? А) Пошаговые инструкции по выполнению задач безопасности Б) Общие руководящие требования по достижению определенного уровня безопасности +С) Широкие, высокоуровневые заявления руководства Г) Детализированные документы по обработке инцидентов безопасности 10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер? А) Анализ рисков +Б) Анализ затрат / выгоды С) Результаты ALE Г) Выявление уязвимостей и угроз, являющихся причиной риска
Навыки: методами выбора элементной базы для построения различных архитектур вычислительных средств;	11.Сложность обеспечения информационной безопасности является следствием: а) злого умысла разработчиков информационных систем +б)объективных проблем современной технологии программирования в)происков западных спецслужб, встраивающих "закладки" в аппаратуру и программы 12.В число универсальных сервисов безопасности входят:

	+а) шифрование б) средства построения виртуальных частных сетей +в) туннелирование 13.В число принципов управления персоналом входят: а)"разделяй и властвуй" +б)разделение обязанностей в)инкапсуляция наследования 14.Комплексное экранирование может обеспечить: +а) разграничение доступа по сетевым адресам +б) выборочное выполнение команд прикладного протокола +в) контроль объема данных, переданных по TCP-соединению 15.Уровень безопасности С, согласно "Оранжевой книге", характеризуется: а) Основы информационной безопасности +б) произвольным управлением доступом в) принудительным управлением доступом г) верифицируемой безопасностью

Таблица 6 ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности - Этап 2

Наименование знаний, умений, навыков и (или) опыта деятельности	Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности
Знать: методы и средства обеспечения информационной безопасности компьютерных систем.	1.Перехват данных является угрозой: а)доступности +б)конфиденциальности в)целостности 2.Что из перечисленного не относится к числу основных аспектов информационной безопасности: а)доступность б)целостность +в)защита от копирования г)конфиденциальность 3.В число целей политики безопасности верхнего уровня входят: +а)формулировка административных решений по важнейшим аспектам б)реализации программы безопасности в)выбор методов аутентификации пользователей +г)обеспечение базы для соблюдения законов и правил 4.В число граней, позволяющих структурировать средства достижения информационной безопасности, входят: +а)законодательные меры б)меры обеспечения доступности в)профилактические меры

	5.Оценка рисков позволяет ответить на следующие вопросы: +а)существующие риски приемлемы? б)кто виноват в том, что риски неприемлемы? +в)что делать, чтобы риски стали приемлемыми?
Уметь: инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем;	6. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании? +А) Поддержка высшего руководства Б) Эффективные защитные меры и методы их внедрения С) Актуальные и адекватные политики и процедуры безопасности Г) Проведение тренингов по безопасности для всех сотрудников 7. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков? А) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски Б) Когда риски не могут быть приняты во внимание по политическим соображениям С) Когда необходимые защитные меры слишком сложны +Г) Когда стоимость контрмер превышает ценность актива и потенциальные потери 8. Что такое политики безопасности? А) Пошаговые инструкции по выполнению задач безопасности Б) Общие руководящие требования по достижению определенного уровня безопасности +С) Широкие, высокоуровневые заявления руководства Г) Детализированные документы по обработке инцидентов безопасности 9. Кто является основным ответственным за определение уровня классификации информации? а) Руководитель среднего звена б) Высшее руководство +в) Владелец г) Пользователь 10. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности? +а) Сотрудники б) Хакеры в) Атакующие г) Контрагенты (лица, работающие по договору)
Навыки: методами защиты информации и конфигурирования комплексных систем	11.В число этапов управления рисками входят: +а)анализ угроз б)угрозы проведения анализа +в)выявление уязвимых мест

защиты.	12.Агрессивное потребление ресурсов является угрозой: +а)доступности б)конфиденциальности в)целостности 13.В рамках программы безопасности нижнего уровня определяются: а)совокупность целей безопасности +б)набор используемых механизмов безопасности в)наиболее вероятные угрозы безопасности 14."Общие критерии" содержат следующие виды требований: +а)функциональные +б)доверия безопасности в)экономической целесообразности 15.В законопроекте "О совершенствовании информационной безопасности" (США, 2001 год) особое внимание обращено на: а)системы электронной коммерции б)инфраструктуру для электронных цифровых подписей +в)средства электронной аутентификации

Таблица 7 ОПК-5 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности - Этап 1

Наименование знаний, умений, навыков и (или) опыта деятельности	Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности
Знать: основные стандарты в области инфокоммуникационных систем и технологий, в том числе стандарты Единой системы программной документации;	1. Кто является основным ответственным за определение уровня классификации информации? а) Руководитель среднего звена б) Высшее руководство +в) Владелец г) Пользователь 2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности? +а) Сотрудники б) Хакеры в) Атакующие г) Контрагенты (лица, работающие по договору) 3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству? а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования б) Требовать подписания специального разрешения каждый

	раз, когда человеку требуется доступ к этой информации +в) Улучшить контроль за безопасностью этой информации г) Снизить уровень классификации этой информации 4. Что самое главное должно продумать руководство при классификации данных? +а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным б) Необходимый уровень доступности, целостности и конфиденциальности в) Оценить уровень риска и отменить контрмеры г) Управление доступом, которое должно защищать данные 5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены? а) Владельцы данных б) Пользователи в) Администраторы +г) Руководство
Уметь: инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем;	6. Что такое процедура? А) Правила использования программного и аппаратного обеспечения в компании +Б) Пошаговая инструкция по выполнению задачи С) Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах Г) Обязательные действия 7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании? +А) Поддержка высшего руководства Б) Эффективные защитные меры и методы их внедрения С) Актуальные и адекватные политики и процедуры безопасности Г) Проведение тренингов по безопасности для всех сотрудников 8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков? А) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски Б) Когда риски не могут быть приняты во внимание по политическим соображениям С) Когда необходимые защитные меры слишком сложны +Г) Когда стоимость контрмер превышает ценность актива и потенциальные потери 9. Что такое политики безопасности? А) Пошаговые инструкции по выполнению задач безопасности Б) Общие руководящие требования по достижению определенного уровня безопасности

	+С) Широкие, высокоуровневые заявления руководства Г) Детализированные документы по обработке инцидентов безопасности 10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер? А) Анализ рисков +Б) Анализ затрат / выгоды С) Результаты ALE Г) Выявление уязвимостей и угроз, являющихся причиной риска
Навыки: методами выбора элементной базы для построения различных архитектур вычислительных средств;	11.Сложность обеспечения информационной безопасности является следствием: а) злого умысла разработчиков информационных систем +б)объективных проблем современной технологии программирования в)происков западных спецслужб, встраивающих "закладки" в аппаратуру и программы 12.В число универсальных сервисов безопасности входят: +а) шифрование б) средства построения виртуальных частных сетей +в) туннелирование 13.В число принципов управления персоналом входят: а)"разделяй и властвуй" +б)разделение обязанностей в)инкапсуляция наследования 14.Комплексное экранирование может обеспечить: +а) разграничение доступа по сетевым адресам +б) выборочное выполнение команд прикладного протокола +в) контроль объема данных, переданных по TCP-соединению 15.Уровень безопасности С, согласно "Оранжевой книге", характеризуется: а) Основы информационной безопасности +б) произвольным управлением доступом в) принудительным управлением доступом г) верифицируемой безопасностью

Таблица 8 ОПК-5 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности - Этап 2

Наименование знаний, умений, навыков и (или) опыта деятельности	Формулировка типового контрольного задания или иного материала, необходимого для оценки знаний, умений, навыков и (или) опыта деятельности

Знать: методы и средства обеспечения информационной безопасности компьютерных систем.	1.Перехват данных является угрозой: а)доступности +б)конфиденциальности в)целостности 2.Что из перечисленного не относится к числу основных аспектов информационной безопасности: а)доступность б)целостность +в)защита от копирования г)конфиденциальность 3.В число целей политики безопасности верхнего уровня входят: +а)формулировка административных решений по важнейшим аспектам б)реализации программы безопасности в)выбор методов аутентификации пользователей +г)обеспечение базы для соблюдения законов и правил 4.В число граней, позволяющих структурировать средства достижения информационной безопасности, входят: +а)законодательные меры б)меры обеспечения доступности в)профилактические меры 5.Оценка рисков позволяет ответить на следующие вопросы: +а)существующие риски приемлемы? б)кто виноват в том, что риски неприемлемы? +в)что делать, чтобы риски стали приемлемыми?
Уметь: инсталлировать, тестировать, испытывать и использовать программно-аппаратные средства вычислительных и информационных систем;	6. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании? +А) Поддержка высшего руководства Б) Эффективные защитные меры и методы их внедрения С) Актуальные и адекватные политики и процедуры безопасности Г) Проведение тренингов по безопасности для всех сотрудников 7. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков? А) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски Б) Когда риски не могут быть приняты во внимание по политическим соображениям С) Когда необходимые защитные меры слишком сложны +Г) Когда стоимость контрмер превышает ценность актива и потенциальные потери 8. Что такое политики безопасности? А) Пошаговые инструкции по выполнению задач безопасности Б) Общие руководящие требования по достижению определенного уровня безопасности +С) Широкие, высокоуровневые заявления руководства Г) Детализированные документы по обработке инцидентов

	безопасности 9. Кто является основным ответственным за определение уровня классификации информации? а) Руководитель среднего звена б) Высшее руководство +в) Владелец г) Пользователь 10. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности? +а) Сотрудники б) Хакеры в) Атакующие г) Контрагенты (лица, работающие по договору)
Навыки: методами защиты информации и конфигурирования комплексных систем защиты.	11.В число этапов управления рисками входят: +а)анализ угроз б)угрозы проведения анализа +в)выявление уязвимых мест 12.Агрессивное потребление ресурсов является угрозой: +а)доступности б)конфиденциальности в)целостности 13.В рамках программы безопасности нижнего уровня определяются: а)совокупность целей безопасности +б)набор используемых механизмов безопасности в)наиболее вероятные угрозы безопасности 14."Общие критерии" содержат следующие виды требований: +а)функциональные +б)доверия безопасности в)экономической целесообразности 15.В законопроекте "О совершенствовании информационной безопасности" (США, 2001 год) особое внимание обращено на: а)системы электронной коммерции б)инфраструктуру для электронных цифровых подписей +в)средства электронной аутентификации

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

В процессе изучения дисциплины предусмотрены следующие формы контроля: текущий, промежуточный контроль (экзамен), контроль самостоятельной работы студентов.

Текущий контроль успеваемости обучающихся осуществляется по всем видам контактной и самостоятельной работы, предусмотренным рабочей программой дисциплины. Текущий контроль успеваемости осуществляется преподавателем, ведущим аудиторные занятия.

Текущий контроль успеваемости может проводиться в следующих формах:

- устная (устный опрос, защита письменной работы, доклад по результатам самостоятельной работы и т.д.);
- письменная (письменный опрос, выполнение, расчетно-проектировочной и расчетно-графической работ и т.д.);
- тестовая (устное, письменное, компьютерное тестирование).

Результаты текущего контроля успеваемости фиксируются в журнале занятий с соблюдением требований по его ведению.

Промежуточная аттестация – это элемент образовательного процесса, призванный определить соответствие уровня и качества знаний, умений и навыков обучающихся, установленным требованиям согласно рабочей программе дисциплины. Промежуточная аттестация осуществляется по результатам текущего контроля.

Конкретный вид промежуточной аттестации по дисциплине определяется рабочим учебным планом и рабочей программой дисциплины.

Зачет, как правило, предполагает проверку усвоения учебного материала практические и семинарских занятий, выполнения лабораторных, расчетно-проектировочных и расчетно-графических работ, курсовых проектов (работ), а также проверку результатов учебной, производственной или преддипломной практик. В отдельных случаях зачеты могут устанавливаться по лекционным курсам, преимущественно описательного характера или тесно связанным с производственной практикой, или имеющим курсовые проекты и работы.

Экзамен, как правило, предполагает проверку учебных достижений обучаемых по всей программе дисциплины и преследует цель оценить полученные теоретические знания, навыки самостоятельной работы, развитие творческого мышления, умения синтезировать полученные знания и их практического применения.

5. Материалы для оценки знаний, умений, навыков и (или) опыта деятельности

Полный комплект оценочных средств для оценки знаний, умений и навыков находится у ведущего преподавателя.