

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»  
*Факультет информатики и информационных технологий*

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

### **Основы управления информационной безопасностью**

Кафедра Информационных технологий и безопасности компьютерных  
систем  
Факультета Информатики и информационных технологий

### **Образовательная программа бакалавриата**

10.03.01 Информационная безопасность

**Направленность (профиль) программы:**  
Безопасность компьютерных систем

**Форма обучения**  
*Очная*

Статус дисциплины:  
*Входит в обязательную часть ОПОП*

Махачкала, 2022

Рабочая программа дисциплины «Основы управления информационной безопасностью» составлена в 2022 году в соответствии с требованиями ФГОС ВО по направлению подготовки 10.03.01\_Информационная безопасность (уровень бакалавриата) от «17» ноября 2020г. №1427.

Разработчик: Гаджиев Амир Маликович кан. физ.мат.н., доцент кафедры информационных технологий и безопасности компьютерных систем

Рабочая программа дисциплины одобрена:  
на заседании кафедры ИТиБКС от «16» марта 2022 г., протокол № 8.

Зав. кафедрой  Ахмедова З.Х.  
(подпись)

на заседании Методической комиссии факультета ИиИТ  
от «14» 03 2022 г., протокол № 7.

/ Председатель  Бакмаев А.Ш.  
(подпись)

Рабочая программа дисциплины согласована с учебно-методическим  
управлением «31» 03 2022г. \_\_\_\_\_

/ Начальник УМУ  Гасангаджиева А.Г.  
(подпись)

### Аннотация рабочей программы дисциплины

Дисциплина «Основы управления информационной безопасностью» является базовой дисциплиной образовательной программы бакалавриата по направлению 10.03.01 «Информационная безопасность».

Дисциплина реализуется на факультете Информатики и ИТ кафедрой Информационных технологий и безопасности компьютерных систем.

Содержание дисциплины охватывает круг вопросов, связанных с изучением современных подходов, методов и методик создания системы управления информационной безопасностью предприятий и организаций, приобретением практических навыков по разработке надежной системы управления информационной безопасности.

Дисциплина нацелена на формирование следующих компетенций выпускника: общепрофессиональных - ОПК-6, ОПК – 10, профессиональных – ПК – 3.

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: *лекции, практические занятия, самостоятельная работа.*

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости в форме *контрольной работы или тестирования* и промежуточный контроль в форме зачета.

Объем дисциплины 2 зачетных единиц, в том числе в академических часах по видам учебных занятий

### Очная форма обучения

Семестр	Учебные занятия						Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен)
	в том числе:						
	всего	Контактная работа обучающихся с преподавателем			СРС, в том числе экзамен		
		всего	Лекции	Лабораторные занятия		Практические занятия	
7	72	42	14	0	28	30	зачет

#### 1. Цели освоения дисциплины

Целями изучения дисциплины «Основы управления информационной безопасностью» является:

*формирование* навыков организации и методологии обеспечения информационной безопасности в коммерческих организациях и организациях банковской системы РФ;

*создание* представления о функциях, структурах и штатах подразделения информационной безопасности; об организационных основах, принципах, методах и технологиях и управлении информационной безопасностью в коммерческих организациях и организациях банковской системы РФ;

*развитие* способностей по использованию существующей системы управления информационной безопасности.

#### 2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина «Основы управления информационной безопасностью» является базовой дисциплиной образовательной программы бакалавриата по направлению 10.03.01 «Информационная безопасность».

Изучение дисциплины базируется на знаниях, полученных студентами при изучении дисциплин «Основы управленческой деятельности», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Программно- аппаратные средства защиты информации», «Защита и обработка конфиденциальных документов». Изучение дисциплины позволяет овладеть

как теоретической базой, так и конкретными практическими навыками по организации и управлению информационной безопасностью.

### 3. Компетенции обучающегося, формируемые в результате освоения дисциплины (перечень планируемых результатов обучения).

Дисциплина «Основы управления информационной безопасностью» обеспечивает инструментарий формирования следующих ОПК и ПК компетенций:

Код и наименование компетенции из ОПОП	Код и наименование индикатора достижения компетенций (в соответствии с ОПОП)	Планируемые результаты обучения	Процедура освоения
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ИД1.ОПК-6.1. Знать: нормативно-правовые основы и документы по проблеме организационного обеспечения информационной безопасности, основные составляющие проблемы и концептуальные положения, угрозы информационной безопасности и меры защиты и противодействия, основные мероприятия по созданию и обеспечению функционирования комплексной системы защиты; требования и рекомендации по защите информации и требования по технической защите информации.	Знает: нормативно-правовые основы и документы по проблеме организационного обеспечения информационной безопасности, основные составляющие проблемы и концептуальные положения, угрозы информационной безопасности и меры защиты и противодействия, основные мероприятия по созданию и обеспечению функционирования комплексной системы защиты; требования и рекомендации по защите информации и требования по технической защите информации	Устный опрос, письменный опрос, практическое занятие.
	ИД2.ОПК-6.2.. Уметь: использовать нормативноправовую базу в решении задач обеспечения информационной безопасности и комплексной защиты информации на предприятии и в организации; строить концептуальные модели информационной безопасности объекта, формулировать основные задачи по созданию и обеспечению функционирования комплексной системы защиты на предприятии, в организации	Умет: использовать нормативно-правовую базу в решении задач обеспечения информационной безопасности и комплексной защиты информации на предприятии и в организации; строить концептуальные модели информационной безопасности объекта, формулировать основные задачи по созданию и обеспечению функционирования	

	ИД3.ОПК-6.3. Владеть: навыками работы с нормативноправовыми и организационнораспорядительными документами в сфере информационной безопасности, вопросами технологии подбора сотрудников и работы с кадрами с точки зрения обеспечения информационной безопасности, основами организации внутри объектового режима.	Должен владеть: навыками работы с нормативноправовыми и организационнораспорядительными документами в сфере информационной безопасности, вопросами технологии подбора сотрудников и работы с кадрами с точки зрения обеспечения информационной безопасности, основами организации внутри объектового режима.	
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их	о специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их ИД 1 ОПК-10.1.Знает программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях ИД 2 ОПК-10.2.Умеет конфигурировать программноаппаратные средства защиты информации в соответствии с заданными политиками безопасности ИД 3 ОПК-10.3. Владеет принципами формирования политики информационной безопасности объекта информатизации	Знает программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях Умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности Владеет принципами формирования политики информационной безопасности объекта информатизации	Устный опрос, письменный опрос, практическое занятие.
ПК-3. Способность готовить презентации, оформлять научно-технические отчеты по результатам выполненной работы, публиковать результаты исследований в виде статей и докладов на научно-технических конференциях	ПК-3.1. Знает современные программные продукты по подготовке презентаций и оформлению научно-технических отчетов ПК-3.2. Умеет готовить презентации и оформлять научные отчеты ПК-3.3. Имеет навыки по подготовке статей и докладов на научно-технических конференциях	Знает: современные программные продукты по подготовке презентаций и оформлению научно-технических отчетов Умеет: готовить презентации и оформлять научные отчеты Имеет навыки по подготовки статей и докладов на научно-технических конференциях	Устный опрос, письменный опрос, практическое занятие.

#### 4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет 5 зачетных единиц, 180 академических часов.

4.2. Структура дисциплины. \_\_\_\_\_

Очная форма обучения

№ п/п	Разделы и темы дисциплины	Семестр	Очная форма обучения				Самостоятельная работа	Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации (по семестрам)
			Лекции	Практические	Лабораторные	СРС		
Модуль 1. Базовые вопросы управления информационной безопасностью								
1.	Основные понятия информационной безопасности	7	1	2	2		2	
2.	Угрозы информационной безопасности в информационных системах	7	2	2	2		4	
3.	Стандарты управления информационной безопасностью	7	3	1	4		4	
4.	Стандарты управления информационной безопасностью	7	4	1	4		2	
5.	Создание СУИБ на предприятии	7	5	2	2		2	
	<i>Итого по модулю 1:</i>		6	8	14		14	Тестирование по мод
Модуль 2 Методы оценки информационных рисков И						НС		
6.	Методика оценки рисков информационной безопасности компании	7	7	2	2		4	
7.	Метод оценки рисков на основе модели информационных потоков	7	8	1			6	
8.	Методики и технологии управления рисками	7	9	1	2		6	
9.	Разработка корпоративной методики анализа рисков	7	10	2	2		6	
	<i>Итого по модулю 2:</i>	7	11	6	14		16	Тестирование по мод
<b>Итого</b>				14	28		30	72

### **4.3. Содержание дисциплины, структурированное по темам (разделам).**

#### **4.3.1. Содержание лекционных занятий по дисциплине**

##### **Модуль 1. Базовые вопросы управления информационной безопасностью**

###### **Тема 1: "Основные понятия информационной безопасности"**

###### **Вопросы:**

1. Понятие информационной безопасности.
2. Основные составляющие информационной безопасности.
3. Управление информационной безопасностью.
4. Важность и сложность проблемы информационной безопасности

###### **Тема 2: "Угрозы информационной безопасности в информационных системах"**

###### **Вопросы:**

1. Основные определения и критерии классификации угроз.
2. Основные угрозы доступности.
3. Основные угрозы целостности.
4. Основные угрозы конфиденциальности.
5. Вредительские программы

###### **Тема 3: «Оценочные стандарты в информационной безопасности» Вопросы:**

1. Роль стандартов ИБ.
2. «Оранжевая книга» как оценочный стандарт.
3. Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем.

###### **Тема 4: «Стандарты управления информационной безопасностью» Вопросы:**

1. Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения.
2. Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасностью. Требования".
3. Сертификация СУИБ на соответствие ISO 27001

###### **Тема 5: "Создание СУИБ на предприятии"**

###### **Вопросы:**

1. Этапы разработки и внедрения системы управления ИБ.
2. Содержание этапов разработки и внедрения системы управления ИБ.

##### **Модуль 2 Методы оценки информационных рисков ИС**

###### **Тема 6: "Методика оценки рисков информационной безопасности компании"**

###### **Вопросы:**

1. Управление рисками. Основные понятия.
2. Метод оценки рисков на основе модели угроз и уязвимостей

###### **Тема 7: «Метод оценки рисков на основе модели информационных потоков»**

###### **Вопросы:**

1. Расчет рисков по угрозе конфиденциальность
2. Расчет рисков по угрозе целостность

###### **Тема 8: Методики и технологии управления рисками**

###### **Вопросы:**

1. Качественные методики управления рисками.
2. Методики COBRA и RA Software Tool.
3. Количественные методики управления рисками.
4. Метод CRAMM.

**Тема 9: "Разработка корпоративной методики анализа рисков" Вопросы:**

1. Постановка задачи
2. Методы оценивания информационных рисков
3. Табличные методы оценки рисков
4. Методика анализа рисков Microsoft

**4.3 .2. Содержание лабораторно-практических занятий по дисциплине.**

**Тема 1. Введение. Базовые вопросы управления ИБ. Процессный подход**

Существующие стандарты и методологии по управлению ИБ: их отличия, сильные и слабые стороны (на примере семейства стандартов ISO/IEC 2700x, СТО БР ИББС-1.0, ГОСТ Р ИСО/МЭК 17799, ГОСТ Р ИСО/МЭК 27001, ISO/IEC 18044, ISO/IEC 25999 и др.).

**Тема 2. Область деятельности СУИБ. Ролевая структура СУИБ. Политика СУИБ**

- Разработка и управление политикой ИБ информационной системы

**Тема 3.Рискология ИБ**

- Анализ модели угроз ИБ и уязвимостей
- Анализ модели информационных потоков

**Тема 4.Основные процессы СУИБ. Обязательная документация СУИБ**

-Процессы улучшения СУИБ («Внутренний аудит», «Корректирующие действия», «Предупреждающие действия»).

- Процесс «Мониторинг эффективности» (включая разработку метрик эффективности). Понятие «Зрелость процесса».

-Процесс «Анализ со стороны высшего руководства». -Процесс «Обучение и обеспечение осведомленности».

**Тема 5.Эксплуатация и независимый аудит СУИБ**

Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. Период эксплуатации СУИБ перед сертификацией. Органы по сертификации, работающие в РФ (их различия и требования). Этапы сертификационного аудита. Решение о сертификации

**Тема 6.Внедрениеразработанных процессов. Документ «Положение о применимости»**

Документирование процесса внедрения разработанных процессов. Типовой документ «Положение о применимости». Цель документа. Структура и содержание документа. Процесс разработки документа, решение спорных ситуаций при разработке документа.

**Тема 7. Процесс «Управление инцидентами ИБ». Процесс «Обеспечение непрерывности ведения бизнеса»**

Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ.

**Тема 8.Обеспечение соответствия требованиям законодательства РФ**



Разработка процессов или дополнение существующих процессов управления ИБ с целью удовлетворения этим требованиям (необходимые документы, процессы, в которых данные требования могут быть выполнены).

№ п/п	№ темы дисциплины	Тематика практических занятий (семинаров)	Технология проведения	Трудоёмкость в часах
1	1-5	Анализ и оценка управленческих и экономических показателей системы управления обеспечением информационной безопасности бизнеса.	Теоретическая справка с кратким изложением основных понятий. Проведение ситуационных моделей происходит в интерактивной форме для отработки навыков управления информационной безопасностью	10
2	6-9	Управление жизненным циклом информационных активов.	Выступления студентов с докладами и презентациями. Аудиторные самостоятельные работы для качественной оценки пройденного материала (15-20 мин.).	8
3	10-13	Анализ влияния информационного риска на деятельность организации.		10
		<b>ИТОГО</b>		28

## 5. Образовательные технологии

Основными образовательными технологиями проведения курса «Основы управления информационной безопасностью» являются:

- Лекции, сопровождаемые компьютерными презентациями;
- практические занятия, в рамках которых составляются и тестируются программы, иллюстрирующие теоретический материал лекций;
- самостоятельная работа студентов, включающая усвоение теоретического материала, поиск дополнительного материала и эффективных способов выполнения заданий, оформление и подготовка к практическому занятию, подготовка к текущему контролю знаний и к итоговому зачету;
- разработанные индивидуальные задания для самостоятельной работы;
- рейтинговая технология контроля учебной деятельности студентов для обеспечения их ритмичной работы в течение семестра
- консультирование студентов по вопросам учебного материала и выполнения курсового задания.

## 6. Учебно-методическое обеспечение самостоятельной работы студентов

При изучении дисциплины «Основы управления информационной безопасностью» обязательными являются следующие виды самостоятельной работы:

- разбор теоретического материала по учебным пособиям и конспектам лекций;
- самостоятельное изучение указанных теоретических вопросов; подготовка к проведению ситуационных моделей в интерактивной форме;

Очная форма

№	Модули и темы	Виды СРС		Объем часов
		обязательные	дополнительные	
<b>Модуль 1</b>				
1.1	Введение. Базовые вопросы управления ИБ. Процессный подход.	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу	Работа с учебной литературой	4
1.2	Область деятельности СУИБ. Ролевая структура СУИБ. Политика СУИБ	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу.	Работа с учебной литературой	6
1.3.	Рискология ИБ	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу подготовка к ответу на коллоквиуме.	Работа с учебной литературой,	4
<b>Всего по модулю 1:</b>				<b>14</b>
<b>Модуль 2</b>				
2.1.	Основные процессы СУИБ. Обязательная документация СУИБ	Конспектирование материала на лекционных занятиях. Подготовка к ответу на семинаре и к докладу.	Работа с учебной литературой	8
2.2	Эксплуатация и независимый аудит СУИБ.	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу, подготовка к ответу на коллоквиуме.	Работа с учебной литературой,	8
<b>Всего по модулю 2:</b>				<b>16</b>
<b>ИТОГО:</b>				<b>30</b>

### ***Контроль результатов освоения дисциплины***

Текущий контроль успеваемости осуществляется путем оценки результатов выполнения заданий лабораторных, самостоятельной работ, посещения лекций.

Промежуточная аттестация осуществляется в форме зачета, который выставляется по результатам проверки выполнения тестов и заданий.

Оценочные средства результатов освоения дисциплины, критерии оценки выполнения заданий представлены в разделе «Фонды оценочных средств для проведения промежуточной аттестации» и фонде оценочных средств образовательной программы.

## **7. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.**

### **7.1. Типовые контрольные задания или иные материалы**

1. Законодательство в области информационной безопасности
2. Криптографические методы и средства защиты информации в компьютерных системах и сетях
3. Политика и модели безопасности
4. Безопасность сетевых операционных систем
5. Безопасность локальных и глобальных сетевых технологий
6. Радиоэлектронные системы и устройства защиты информации
7. Комплексная защита информации в компьютерных системах и сетях Актуальность проблем информационной безопасности в современном мире.
8. Задачи и методы обеспечения информационной безопасности в сфере внешней и внутренней политики России.
9. Информация - наиболее ценный ресурс современного общества.
10. Проблемы информационных войн на современном этапе.
11. Государственная информационная политика РФ.
12. Государственная система правового обеспечения защиты информации в РФ.
13. Государственное регулирование использования криптографических средств.
14. Государственное регулирование использования электронной цифровой подписи.
15. Информационная безопасность в государственной информационной политике РФ.
16. Информация как объект юридической защиты.
17. Информационное право на современном этапе развития общества.
18. Задачи и принципы организации службы информационной безопасности предприятий.
19. Зарубежное законодательство в области информационной безопасности.
20. Зарубежные стандарты в области информационной безопасности.
21. Информационная безопасность беспроводных сетей.
22. Информационная безопасность компьютерных сетей.
23. Современное информационное оружие и его классификация.
24. Информация как наиболее ценный ресурс современного общества.
25. Категории информации по режиму ограничения доступа и использования.
26. Лицензирование, сертификация и аттестация объектов информатизации и защиты информации.
27. Использование криптографических и стеганографических методов в информационном обмене.
28. Международные стандарты информационного обмена.
29. Обеспечение информационной безопасности в Internet.
30. Основные положения Доктрины информационной безопасности.
31. Отечественные стандарты в области информационной безопасности.
32. Оценка безопасности информационных технологий.
33. Организационная структура государственной системы обеспечения информационной безопасности РФ.
34. Базовые источники системы информационной безопасности.
35. Правонарушения и ответственность в области эксплуатации информационных систем и информационной безопасности.
36. Правовая основа системы информационной безопасности.
37. Нормативно-правовое обеспечение в сфере связи и коммуникаций.
38. Корпоративная политика информационной безопасности.

39. Проблемы информационной безопасности в национальном и международном аспектах.
40. Проблемы информационной безопасности в области государственного и муниципального управления.
41. Программно-технический уровень информационной безопасности.
42. Современное состояние нормативно-правовой базы информационной безопасности.
43. Система подготовки кадров в области информационной безопасности в РФ.
44. Угрозы безопасности информации и информационные атаки.
45. Угрозы информационной безопасности в компьютерных сетях.
46. Управление информационными рисками.
47. Электронная цифровая подпись - правовой и технический

### **Типовые контрольные задания**

1. Под угрозой безопасности информации в компьютерной системе (КС) понимают:
2. Уязвимость информации — это: \_\_\_\_\_
3. Атакой на КС называют: \_\_\_\_\_
4. Искусственные угрозы исходя из их мотивов разделяются на:
5. непреднамеренным угрозам относятся: \_\_\_\_\_
6. К умышленным угрозам относятся: \_\_\_\_\_
7. Косвенными каналами утечки называют: \_\_\_\_\_
8. К косвенным каналам утечки информации относятся: \_\_\_\_\_
9. Непосредственными каналами утечки называют: \_\_\_\_\_
10. К непосредственным каналам утечки информации относятся:
11. Избирательная политика безопасности подразумевает, что:
12. Полномочная политика безопасности подразумевает, что:
13. Достоверная вычислительная база - это: \_\_\_\_\_
14. Достоверная вычислительная база выполняет задачи: \_\_\_\_\_
15. Уязвимость информации — это: \_\_\_\_\_
16. Идентификация объекта - это: \_\_\_\_\_
17. Параллельная схема идентификации позволяет увеличить:
18. Какие существуют формы представления объектов, аутентифицирующих пользователя:
19. Внешняя и внутренняя формы представления аутентифицирующего объекта должны быть:
20. Внешние объекты могут быть технически реализованы на различных носителях информации?
21. Для чего были разработаны протоколы идентификации с нулевой передачей знаний:
22. Механизм запроса-ответа используется для: \_\_\_\_\_
23. Кто разработал алгоритм идентификации с нулевой передачей знания:
24. Схему идентификации с нулевой передачей знаний предложили:
25. Для чего создается система разграничения доступа к информации:
26. Сбои, отказы технических и программных средств могут быть использованы для НСД?
27. Правильность функционирования ядра безопасности доказывается путем:
28. Мандатное управление позволяет упростить процесс регулирования доступа?
29. Матричное управление доступом предполагает использование:

30. Основной проблемой создания высокоэффективной защиты от НСД является:
31. Аппаратно-программные средства криптографической защиты информации выполняют функции:
32. Надежность защиты информации в компьютерной системе определяется:
33. Использование аппаратных средств снимает проблему: \_\_\_\_\_
34. Криптографические функции плат КРИПТОН образующие ядро системы безопасности реализуются
35. К частично контролируемым компьютерным системам можно отнести современные КС, использующие:
36. Безопасность в частично контролируемых компьютерных системах может быть обеспечена:
37. К основным компонентам сети относятся: \_\_\_\_\_
38. В качестве ключевых носителей устройств криптографической защиты
39. данных серии КРИПТОН используются: \_\_\_\_\_
40. Средства серии КРИПТОН независимо от операционной среды
41. обеспечивают: \_\_\_\_\_
42. В системе Secret Disk используется: \_\_\_\_\_
43. В чем заключается особенность системы Secret Disk: \_\_\_\_\_
44. Мастер-ключ в Устройствах криптографической защиты данных серии
45. КРИПТОН загружается: \_\_\_\_\_
46. Криптографических функций в устройствах криптографической защиты
47. данных серии КРИПТОН выполняются: \_\_\_\_\_
48. Абонентские места, персональные компьютеры или терминалы клиента являются основными компонентами сети?
49. Возможные каналы утечки информации по классификации разделяют:
50. К группе каналов утечки информации в которой основным средством
51. является человек, относятся следующие утечки: \_\_\_\_\_
52. К группе каналов утечки информации в которой основным средством
53. является аппаратура, относятся следующие утечки: \_\_\_\_\_
54. К группе каналов утечки информации в которой основным средством
55. является программа, относятся следующие утечки: \_\_\_\_\_
56. К средствам активной защиты относятся: \_\_\_\_\_
57. К средствам пассивной защиты относятся: \_\_\_\_\_
58. К средствам собственной защиты относятся: \_\_\_\_\_
59. Может ли информативный сигнал в сети электропитания быть каналом утечки информации?
60. Мероприятия по инженерно-технической защите информации от утечки по электромагнитному каналу подразделяются на:
61. Технические мероприятия направлены: \_\_\_\_\_
62. Организационными мероприятиями предусматривается: \_\_\_\_\_
63. Активные способы защиты информации при ее утечке через сеть
64. электропитания направлены на: \_\_\_\_\_
65. Пассивные способы защиты информации при ее утечке через сеть
66. электропитания направлены на: \_\_\_\_\_
67. Для минимизации паразитных связей внутри ПЭВМ используются:
68. Под системой защиты от несанкционированного использования и

69. копирования понимается \_\_\_\_
70. Под надежностью системы защиты от несанкционированного
71. копирования понимается:
72. Методы, затрудняющие считывание скопированной информации
73. основываются на: \_\_\_\_
74. Для защиты от несанкционированного использования программ могут применяться электронные ключи?
75. Мероприятия по инженерно-технической защите информации от утечки
76. по электромагнитному каналу подразделяются на: \_\_\_\_\_
77. Любая криптографическая система основана на использовании:
78. В симметричной криптосистеме отправитель и получатель сообщения
79. используют: \_\_\_\_
80. Асимметричная криптосистема предполагает использование:
81. Под ключевой информацией понимают: \_\_\_\_\_
82. В каких режимах может выполняться изучение логики работы

### **Критерии оценки:**

- оценка «отлично» выставляется студенту, если полностью владеет как теоретическими знаниями, так и практическими навыками, отвечает на поставленные вопросы
- оценка «хорошо» - владеет теоретическими знаниями, обладает практическими навыками, затрудняется ответить на поставленные вопросы
- оценка «удовлетворительно» владеет только основами теоретического аспекта разбираемой темы
- оценка «неудовлетворительно» не обладает ни теоретическими знаниями, ни практическими навыками, не отвечает на контрольные вопросы

### **Перечень вопросов к зачету (7 семестр).**

1. Основные функции подсистемы защиты ОС.
2. Базовая политика безопасности.
3. Специализированные политики безопасности.
4. Избирательная и полномочная политика безопасности.
5. Процедуры безопасности.
6. Разработка политики безопасной организации.
7. Управление информационными потоками.
8. Достоверная вычислительная база.
9. Механизмы защиты ДВБ.
10. Принципы реализации политики безопасности.
11. Основные критерии оценки безопасности систем.
12. Роли и ответственность в безопасности сети.
13. Идентификация и аутентификация пользователя.
14. Аутентификация на основе многоцветных паролей.
15. Аутентификация на основе одноразовых паролей.
16. Строгая аутентификация. Основные понятия.
17. Типовые схемы идентификации и аутентификации пользователя.
18. Взаимная проверка подлинности пользователей.

19. Упрощенная схема идентификации с нулевой передачей знаний.
  20. Параллельная схема идентификации с нулевой передачей знаний.
  21. Схема идентификации Гиллоу-Куискуотера.
  22. Защита информации в КС от несанкционированного доступа.
  23. Управление доступом (Система разграничения доступа к информации в КС).
  24. Состав системы разграничения доступа (Система разграничения доступа к информации в КС).
  25. Концепция построения систем разграничения доступа.
  26. Организация доступа к ресурсам КС.
  27. Обеспечение целостности и доступности информации в КС.
  28. Основные понятия криптографической защиты информации.
  29. Симметричные криптосистемы шифрования.
  30. Асимметричные криптосистемы шифрования.
  31. Функции хеширования.
  32. Электронная цифровая подпись.
  33. Управление криптоключами.
  34. Корпоративная информационная системы.
  35. Архитектура «облачных сервисов».
  36. Подсистемы информационной безопасности традиционных КИС.
  37. Средства защиты в виртуальных средах.
  38. Обеспечение безопасности «облачных» сред на базе пакета Trend Micro Deep Security.
  39. Защита на канальном уровне. Протокол PPTP.
  40. Защита на канальном уровне. Протокол L2TP.
  41. Защита на сетевом уровне. Архитектура средств безопасности IPSec.
  42. Защита передаваемых данных с помощью протоколов AH и ESP.
  43. Протокол управления криптоключами IKE.
  44. База данных SAD и SPD.
  45. Особенности реализации средств IPSec и их преимущества.
  46. Протоколы SSL и TLS.
  47. Протокол SOCKS.
  48. Особенности безопасности беспроводных сетей.
  49. Функции межсетевых экранов.
  50. Фильтрация трафика (технологии межсетевого экранирования).
  51. Выполнение функций посредничества.
  52. Межсетевые экраны.
  53. Классификация сети VPN и Средства обеспечения безопасности VPN.
  54. Функционирование системы управления доступом.
  55. Аутентификации удаленных пользователей на основе одноразовых паролей
- ОТР.
56. Протоколы аутентификации удаленных пользователей. Протокол PAP.
  57. Протоколы аутентификации удаленных пользователей. Протокол CHAP.
  58. Протоколы аутентификации удаленных пользователей. Протокол EAP.
  59. Протоколы аутентификации удаленных пользователей. Протокол S/Key.
  60. Протоколы аутентификации удаленных пользователей. Протокол Kerberos.

**7.2. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.**

Фонд оценочных средств дисциплины включает в себя контрольные вопросы, задания контрольных работ, вопросы для промежуточной аттестации.

Виды самостоятельной работы обучающихся

Изучение основной и дополнительной литературы по материалам курса.

Выполнение заданий самостоятельной работы по курсу.

Таблица 1.1 Таблица максимальных баллов по видам учебной деятельности

1	2	3	4	5	6	7	8	9
Се местр	Лекции	Лабораторные занятия	Практические занятия	Самостоятельная работа	Автоматизированное тестирование	Другие виды учебной деятельности	Промежуточная аттестация	Итого
3	5	0	15	35	0	5	40	100

Программа оценивания учебной деятельности студента Семестр 7

**Лекции.** Посещаемость, опрос, активность за семестр — от 0 до 5 баллов.

**Лабораторные занятия. Выполнение одной лабораторной работы – 10б.**

**Практические занятия.** Посещаемость, опрос, активность за семестр — от 0 до 15 баллов.

Самостоятельная работа.

Контроль выполнения заданий самостоятельной работы в течение одного семестра — от 0 до 25 баллов;

Контрольная работа (от 0 до 10 баллов);

Таким образом, студент в течении 3-го семестра может получить от 0 до 35 баллов.

Автоматизированное тестирование. **Не предусмотрено.**

**Другие виды учебной деятельности.**

Написание реферата является одной из форм обучения студентов. Данная форма обучения направлена на организацию и повышение уровня самостоятельной работы студентов. Реферат, как форма обучения студентов - это краткий обзор максимального количества доступных публикаций по заданной теме, подготовка самого реферативного обзора и презентации по нему. При проведении обзора должна проводиться и исследовательская работа, но объем ее ограничен, так как анализируется уже сделанные выводы и в связи с небольшим объемом данной формы работы. Преподавателю предоставляется сам реферат в письменной форме (электронная версия в формате Microsoft Word) и презентация к нему (электронная версия в формате PowerPoint). Сдача реферата происходит в форме защиты доклада с использованием подготовленной презентации.

**Промежуточная аттестация.** Методика оценивания знаний обучающихся по дисциплине «Облачные технологии» в ходе промежуточной аттестации:

25-40 баллов:



Ответ студента содержит:

глубокое знание программного материала, а также основного содержания и новаций лекционного курса по сравнению с учебной литературой;

знание концептуально-понятийного аппарата всего курса;

знание монографической литературы по курсу,

также свидетельствует о способности:

самостоятельно критически оценивать основные положения курса;

увязывать теорию с практикой.

15-24 баллов:

Ответ студента свидетельствует:

о полном знании материала по программе;

о знании рекомендованной литературы,

а также содержит в целом правильное, но не всегда точное и аргументированное изложение материала.

1-14 баллов:

Ответ студента содержит:

поверхностные знания важнейших разделов программы и содержания лекционного курса;

затруднения с использованием научно-понятийного аппарата и терминологии курса;

стремление логически четко построить ответ, а также свидетельствует о возможности последующего обучения.

Студенту, имеющему существенные пробелы в знании основного материала по программе, а также допустившему принципиальные ошибки при изложении материала ставится оценка 0 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за один семестр по дисциплине «Облачные технологии» составляет 100 баллов.

Итоговой формой контроля знаний, умений и навыков по дисциплине является **зачет**. Зачет проводится в форме тестирования. При соответствии ответа учащегося на зачете более чем 51 % критериев из этого списка выставляется оценка «удовлетворительно», 66% – 85% оценка «хорошо», 86% и выше оценка «отлично».

## **8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.**

### **а) основная литература:**

1. **Правовое обеспечение информационной безопасности** : [учеб. пособие для вузов по специальностям 075200 "Компьютер. безопасность", 075500 "Комплекс. обеспечение информ. безопасности и автоматизир. систем", 075600 "Информ. безопасность телекоммуникац. систем" / С.Я.Казанцев и др.]; под ред. С.Я.Казанцева. - М. : Academia, 2005. - 239 с. : ил. ; 22 см. - (Высшее профессиональное образование. Информационная безопасность). - Библиогр.: с. 235-237. - Допущено УМО. - ISBN 5-7695-1209-1 : 129-47

2. **Филин С. А.** Информационная безопасность : учеб. пособие / Филин, Сергей Александрович. - М. : Альфа-Пресс, 2006. - 411 с. - ISBN 5-94280-163-0 : 129-03.

3. **Галатенко В. А.** Стандарты информационной безопасности : курс лекций: учеб. пособие / Галатенко, Владимир Антонович ; под ред. В.Б.Бетелина; Интернет-ун-т информ. технологий. - 2-е изд. - М. : ИНТУИТ.ру, 2006. - 263 с. - (Основы информационных технологий). - ISBN 5-9556-0053-1 : 176-00.

4. **Уколов В. Ф.** Теория управления : учеб. для вузов / Уколов, Владимир Фёдорович, А. М. Масс, И. К. Быстрыков. - 3-е изд., доп. - М. : Экономика, 2007. - 696 с. - Допущено МО РФ. - ISBN 978-5-282-02698-6 : 260-00

5. **Галатенко В. А.** Основы информационной безопасности : учеб. пособие для студентов вузов, обуч. по специальности 351400 "Прикл. информ." / Галатенко, Владимир Антонович. - 4-е изд. - М. : Изд-во Интернет-Ун-та Информ. Технологий: БИНОМ. Лаб. знаний, 2016, 2008, 2006. - 205 с. - (Основы информационных технологий). - Рекомендовано УМО. - ISBN 978-5-94774-821-5 : 230-00.

6. Петров С. В. Информационная безопасность : учеб. пособие /. - Новосибирск: М. : АРТА, 2012. - 439-77.

**б)дополнительная:**

1. ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems - Requirements.Международный стандарт. ISO/IEC 27000:2005 Информационные технологии. Методы обеспечения безопасности. Определения и основные принципы./ <http://www.27000.org/>

2. Аудит информационной безопасности. Под ред. А.П.Курило. - М: БДЦ-Пресс, 2014.

3. Международный стандарт. ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования (BS 7799-2:2005)./ <http://www.27000.org/>

4. Международный стандарт. ISO/IEC 27002:2005 Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью./ <http://www.27000.org/>Международный стандарт. ISO/IEC 27003:2005 Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы управления информационной безопасностью./ <http://www.27000.org/>

5. Международный стандарт. ISO/IEC 27004:2005 Информационные технологии. Методы обеспечения безопасности. Измерение эффективности системы управления информационной безопасностью./ <http://www.27000.org/>

6. Международный стандарт. ISO/IEC 27005:2005 Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности./ <http://www.27000.org/>

7. Международный стандарт. ISO/IEC 27006:2005 Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью./ <http://www.27000.org/>

8. Международный стандарт. ISO/IEC 27007:2005 Информационные технологии. Методы обеспечения безопасности. Руководство для аудитора систем управления информационной безопасностью./ <http://www.27000.org/>

9. Петренко С., Симонов С. Управление информационными рисками. Экономически оправданная безопасность. — М.: АйТи-Пресс, 2012.

10. Петренко С.А., Курбатов В.А. Политики информационной безопасности. - М.: ДМК пресс, 2013.

14

11. Репин В., Елиферов В. Процессный подход к управлению. Моделирование бизнес-процессов. М.: Стандарты и качество, 2014.

12. Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение информационной безопасности. - М.: Академия, 2008 г. - 192 стр.

13. Золотарев Управление информационной безопасностью. Ч. 1. Анализ информационных рисков - Красноярск: Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева, 2010.

**9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.**

1. ЭБС IPRbooks: <http://www.iprbookshop.ru/>
2. Электронно-библиотечная система «Университетская библиотека онлайн»(архив):[www.dub.m](http://www.dub.m)
3. Единое окно доступа к образовательным ресурсам. <http://window.edu.ru/>
4. <http://www.microsoft.com/msf>
5. <http://www.uml.org>
6. <http://www.wikipedia.org>

**10. Методические указания для обучающихся по освоению дисциплины. Критерии и показатели сформированности компетенций**

Степень (уровень) сформированности компетенций на этапе изучения дисциплины «Основы управления информационной безопасностью» оценивается по следующим критериям: мотивационно-ценностный, когнитивный, операционно-деятельностный. Показателями критериев являются результаты обучения по дисциплине (дескрипторы) таблицы 1. Инструментарий, этапы измерения показателей и критериев компетенции представлены в таблице.

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ**

Этапы контроля: раздел 2 (самостоятельная работа), раздел 3 (самостоятельная работа), раздел 4

(самостоятельная работа), раздел 5 (самостоятельная работа), раздел 6 (самостоятельная работа),

раздел 7 (самостоятельная работа), зачет.

Время на выполнение: 60 мин.

Метод оценивания: автоматизированный

Критерии оценки результатов выполнения: менее 50% правильных ответов - неудовлетворительно, менее 65% - удовлетворительно, менее 86% хорошо, 86% и более - отлично.

**11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и**

**информационных справочных систем.**

*Информационные технологии* Образовательный процесс осуществляется с применением локальных и распределенных информационных технологий (таблица 4, 5).

Таблица 4 - Локальные информационные технологии

Группа программных средств	Наименование программного продукта
Офисные программы	Microsoft Office
	Libre Office
Средства разработки	MicroSoft Visual Studio 2015 MicroSoft SQL Server 2012 VipNet Client 4 Dallas Lock 8.0 КриптоПро CSP

Таблица 5 - Распределенные информационные технологии

Группа	Наименование
Система тестирования	Система сетевого компьютерного тестирования ДГУ <a href="http://www.ts.icc.dgu.ru">www.ts.icc.dgu.ru</a>
Библиотеки и образовательные ресурсы	Электронная библиотека ДГУ <a href="http://www.elib.dgu.ru">http://www.elib.dgu.ru</a>
	Кафедральные сайты ДГУ <a href="http://cafedra.dgu.ru">http://cafedra.dgu.ru</a>
	Сайте электронных образовательных ресурсов ДГУ <a href="http://eor.dgu.ru">http://eor.dgu.ru</a>
Система электронного обучения	Сервер электронного обучения moodle <a href="http://moodle.dgu.ru">http://moodle.dgu.ru</a>

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

Таблица 6 - Материально-техническая база

Помещения для осуществления образовательного процесса	Перечень основного оборудования (с указанием кол-ва посадочных мест)	Адрес (местоположение)
Аудитории для проведения лекционных занятий		
Лекционные аудитории	Интерактивная доска, ноутбук; проектор. Количество посадочных мест - 30.	Ауд. 3-14, 4-16, 210, учебный корпус № 8, г.Махачкала, ул. Держинского, 12.
Аудитории для проведения лабораторных занятий, контроля успеваемости		
Компьютерный класс	Компьютеры с выходом в Интернет и доступом в электронную информационно-образовательную среду вуза. Количество посадочных мест - 15.	Компьютерный зал № 2 учебный корпус № 3, г.Махачкала, ул. Держинского, 12.
Помещения для самостоятельной работы		
Компьютерные классы	Компьютеры с выходом в Интернет и доступом в электронную информационно-образовательную среду вуза. Количество посадочных мест - 15	Компьютерный зал № 1, учебный корпус № 3, г. Махачкала, ул. Держинского, 12.
Читальный зал библиотеки ДГУ	Компьютеры с выходом в Интернет и доступом в электронную информационно-образовательную среду вуза. Количество посадочных мест - 30.	Электронный читальный зал научной библиотеки ДГУ, г. Махачкала, ул. Батырая, 4