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 **_Информатики и информационных технологий**

Образовательная программа по направлению

10.03.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Профиль подготовки

БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ

Уровень высшего образования
Бакалавриат

Форма обучения
очная

Статус дисциплины:
базовая

Махачкала 2018

Рабочая программа дисциплины **«Основы управления информационной безопасностью»** составлена в 2018 году в соответствии с требованиями ФГОС ВО по направлению подготовки **10.03.01 «Информационная безопасность»**, уровень Бакалавриат, утвержденного приказом Министерства образования и науки от 1 декабря 2016 г, № 1515, вступил в силу 20 декабря 2016 г.

Разработчик: Абдуллаев Габид Шаванович, к.э.н., доцент кафедры информатики и информационных технологий

Рабочая программа дисциплины одобрена:

На заседании кафедры ИиИТ от «2» 07 2018г., протокол № 12

Зав. Кафедрой _____ Ахмедов С.А.

(подпись)

На заседании Методической комиссии факультета ИиИТ

от «3» июня 2018г., протокол № 10.

Председатель _____ Камилов К.Б.

(подпись)

Рабочая программа дисциплины согласована с учебно – методическим управлением «04» 07 2018г. _____

(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 Информатики и ИТ.

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: общекультурных – ОК-4; общепрофессиональных – ОПК-5, ОПК – 7.

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 3 зачетных единиц, в том числе в академических часах по видам учебных занятий

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	из них						
			Лекции	Лабораторные занятия	Практические занятия	КСР	консультации		
7	108	50	36	-	18	2	2	50	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 бакалавлиата

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 ОК и ОПК компетенций:

Код компетенции из ФГОС ВО	Наименование компетенции из ФГОС ВО	Планируемые результаты обучения
ОК-4	способностью использовать основы правовых знаний в различных сферах деятельности	Знает: основы российской правовой системы и законодательства; права, свободы и обязанности человека и гражданина; организацию судебных, правоприменительных и правоохранительных органов; правовые нормы действующего законодательства, регулирующие отношения в различных сферах жизнедеятельности; основные положения и нормы конституционного, гражданского, семейного, трудового, административного и уголовного права. Умеет защищать гражданские права; использовать нормативно-правовые знания в различных сферах жизнедеятельности. Владеет: навыками поиска и анализа нормативных актов, регулирующих отношения в различных сферах жизнедеятельности; навыками реализации и защиты своих прав.
ОПК-5	способностью использовать нормативные правовые акты в профессиональной деятельности	Знает: основные понятия, цели, принципы, сферы применения, объекты, субъекты, правовые основы профессиональной деятельности, ее составляющих элементов, методы и средства правовой защиты интересов субъектов. Умеет: использовать в практической деятельности правовые знания; анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности, ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности и использовать их в своей деятельности, предвидеть юридические опасности и угрозы и соблюдать основные правовые требования информационной безопасности. Владеет: основами правового мышления, навыками самостоятельного анализа правовой информации, анализа юридических последствий, связанных с использованием информации, навыками работы с нормативными правовыми актами, нормативной и технической

		информацией, необходимой для профессиональной деятельности, навыками поиска нормативной правовой информации необходимой для профессиональной деятельности
ОПК-7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Знает: о критериях, которым должно соответствовать информационное общество, о соответствии современного общества этим критериям. Знать периоды развития информационной безопасности, этапы развития вычислительной техники, критерии периодизации, развитие элементной базы, ведущих ученых в этой области, развитие отечественной вычислительной техники и информационной безопасности в России. Умеет: осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе мораль но-нравственных и правовых норм, соблюдать принципы профессиональной этики. Владеет: навыками: проводить поиск информации по требуемой тематике, аргументировано и последовательно излагать свое мнение, проводить сравнительный анализ состояния общества и вычислительной техники. Обладать способностью к логически правильному мышлению, обобщению, анализу, критическому осмыслению информации, систематизации, прогнозированию, постановке исследовательских задач и выбору путей их решения на основании принципов научного познания.

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет 3 зачетных единиц, 108 академических часов.

4.2. Структура дисциплины.

№ п/п	Разделы и темы дисциплины	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Самостоятельная работа	Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
			Лекции	Практические	Лаборат.занятия	СРС		
Модуль 1. Базовые вопросы управления информационной безопасностью								
1.	Основные понятия информационной безопасности	7	2				2	

2.	Угрозы информационной безопасности в информационных системах	7	2	2			4	
3.	Стандарты управления информационной безопасностью	7	4				4	
4.	Стандарты управления информационной безопасностью	7	2	2			4	
5.	Создание СУИБ на предприятии	7	2	2			4	
	Всего		12	6			18	Тестирование по мод
Модуль 2 Методы оценки информационных рисков ИС								
6.	Методика оценки рисков информационной безопасности компании	7	4	2			4	
7.	Метод оценки рисков на основе модели информационных потоков	7	2				4	
8.	Методики и технологии управления рисками	7	4	2			4	
9.	Разработка корпоративной методики анализа рисков	7	2	2			6	
	Всего		12	6			18	Тестирование по мод
Модуль 3 Современные методы и средства обеспечения ИБ								
10.	Современные методы и средства анализа и управление рисками информационных систем компаний	7	4	2			4	
11.	Правовое обеспечение ИБ	7	2				4	
12.	Организационные меры обеспечения безопасности компьютерных информационных систем	7	2	2			6	
13.	Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом "	7	4	2			4	
	Всего		12	6			18	Тестирование по мод
Итого по курсу			**36**	**18**			**54**	**экзамен**

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 безопасности. 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**

Модуль 3 Современные методы и средства обеспечения ИБ

Тема 10: " Современные методы и средства анализа и управление рисками информационных систем компаний"

Вопросы:
1. Обоснование необходимости инвестиций в информационную безопасность компании.
2. Методика FRAP (фреп).
3. Методика OCTAVE (октэйв)
4. Методика Risk Watch (риск вэтч).

Тема 11: «Правовые меры обеспечения безопасности компьютерных информационных систем»

Вопросы:
1. Обзор российского законодательства в области информационной безопасности
2. Закон "Об информации, информатизации и защите информации"
3. Другие законы и нормативные акты
4. О текущем состоянии российского законодательства в области информационной безопасности
5. Обзор зарубежного законодательства в области информационной безопасности

Тема 12: «Организационные меры обеспечения безопасности компьютерных информационных систем»

Вопросы
1. Общие положения организационной защиты.
2. Особенности организационной защиты компьютерных информационных систем и сетей.
3. Управление информационной безопасности предприятия.

Тема 13: «Программно-технические меры обеспечения безопасности компьютерных информационных систем»

Вопросы:
1. Основные программно-технические меры.
2. Идентификация и аутентификация.
3. Управление доступом.

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.Внедрение разработанных 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 дисцип-лины	Тематика практических занятий (семинаров)	Технология проведения	Трудоём-кость 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	6

2	**6-9**	Управление жизненным циклом информационных активов.	интерактивной форме для отработки навыков управления информационной безопасностью Выступления студентов с докладами и презентациями. Аудиторные самостоятельные работы для качественной оценки пройденного материала (15-20 мин.).	6
3	**10-13**	Анализ влияния информационного риска на деятельность организации.		6
		ИТОГО		18

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 экзамену;
- 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 заданий.

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;

№	Модули и темы	Виды СРС		Объем часов
		обязательные	дополнитель-ные	
Модуль 1				
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	6

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,	6
	Всего по модулю 1:			**18**
Модуль 2				
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,	10
	Всего по модулю 2:			**18**
Модуль 3				
3.1	Внедрение разработанных процессов. Документ «Положение о применимости»	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу	Работа с учебной литературой,	6
3.2	Процесс «Управление инцидентами ИБ. Процесс «Обеспечение непрерывности ведения бизнеса»	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу	Работа с учебной литературой, выполнение расчетной работы на компьютере	6
3.3	Обеспечение соответствия требованиям законодательства РФ	Конспектирование материала на лекционных занятиях. подготовка к ответу на семинаре и к докладу подготовка к ответу на коллоквиуме.	Работа с учебной литературой,.	6
	Всего по модулю 3:			**18**
	ИТОГО:			**54**

Контроль результатов освоения дисциплины

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

Промежуточная аттестация осуществляется в форме экзамена, 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. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

Перечень компетенций с указанием этапов их формирования приведен в описании образовательной программы.

Код компетенции из ФГОС ВО	Наименование компетенции из ФГОС ВО	Планируемые результаты обучения	Процедура освоения
ОК-4	способностью использовать основы правовых знаний в различных сферах деятельности	Знает: основы российской правовой системы и законодательства; права, свободы и обязанности человека и гражданина; организацию судебных, правоприменительных и правоохранительных органов; правовые нормы действующего законодательства, регулирующие отношения в различных сферах жизнедеятельности; основные положения и нормы конституционного, гражданского, семейного, трудового, административного и уголовного права. Умеет защищать гражданские права; использовать нормативно-правовые знания в различных сферах жизнедеятельности. Владеет: навыками поиска и анализа нормативных актов, регулирующих отношения в различных сферах жизнедеятельности; навыками реализации и защиты своих прав.	Устный опрос, письменный опрос
ОПК-5	способностью использовать нормативные правовые акты в профессиональной деятельности	Знает: основные понятия, цели, принципы, сферы применения, объекты, субъекты, правовые основы профессиональной деятельности, ее составляющих элементов, методы и средства правовой защиты интересов субъектов. Умеет: использовать в практической деятельности правовые знания; анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности, ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности и использовать их в своей деятельности, предвидеть юридические опасности и угрозы и соблюдать основные правовые требования информационной безопасности. Владеет: основами правового мышления, навыками самостоятельного анализа правовой информации, анализа юридических последствий, связанных с использованием информации, навыками работы с нормативными правовыми актами, нормативной и технической информацией, необходимой для профессиональной деятельности, навыками поиска нормативной	Устный опрос, письменный опрос

		правовой информации необходимой для профессиональной деятельности	
ОПК-7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Знает: о критериях, которым должно соответствовать информационное общество, о соответствии современного общества этим критериям. Знать периоды развития информационной безопасности, этапы развития вычислительной техники, критерии периодизации, развитие элементной базы, ведущих ученых в этой области, развитие отечественной вычислительной техники и информационной безопасности в России. Умеет: осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе мораль но-нравственных и правовых норм, соблюдать принципы профессиональной этики. Владеет: навыками: проводить поиск информации по требуемой тематике, аргументировано и последовательно излагать свое мнение, проводить сравнительный анализ состояния общества и вычислительной техники. Обладать способностью к логически правильному мышлению, обобщению, анализу, критическому осмыслению информации, систематизации, прогнозированию, постановке исследовательских задач и выбору путей их решения на основании принципов научного познания.	Устный опрос, письменный опрос

7.2. Типовые контрольные задания

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

Общий результат выводится как интегральная оценка, складывающая из текущего контроля - 30% и промежуточного контроля - 70%.

Текущий контроль по дисциплине включает:

- посещение занятий - _0__ баллов,
- участие на практических занятиях - 20 баллов,
- выполнение лабораторных заданий – 60 баллов,
- выполнение домашних (аудиторных) контрольных работ – 20 баллов.

Промежуточный контроль по дисциплине включает:

- устный опрос - 30 баллов,
- письменная контрольная работа - 30 баллов,
- тестирование - 40 баллов.

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. Быстряков. - 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.

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.biblioclub.ru
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.

Критерии сформированности компетенции	Способы оценки	
	Этапы контроля	Средства оценки
Мотивационно-ценностный критерий	4, 6, 7, экзамен	1
Когнитивный критерий	4, 5, 6, 7	1
Операционно-деятельностный критерий	4, 5, 7	1
	6, экзамен	
Интегральная оценка	Экзамен	1

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), экзамен.
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
Распознавание текста и речи	ABBYY FineReader 2010
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 www.ts.icc.dgu.ru
Библиотеки и образовательные ресурсы	Электронная библиотека ДГУ http://www.elib.dgu.ru
	Кафедральные сайты ДГУ http://cafedra.dgu.ru
	Сайте электронных образовательных ресурсов ДГУ http://eor.dgu.ru
Система электронного обучения	Сервер электронного обучения moodle http://moodle.dgu.ru

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, 2-10, учебный корпус № 8, г.Махачкала, ул. Джержинского, 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. Джержинского, 12.
Помещения для самостоятельной работы		
Компьютерные классы	Компьютеры с выходом в Интернет и доступом в электронную информационно-	Компьютерный зал № 1, учебный

	образовательную среду вуза. Количество посадочных мест – 15	корпус № 3, г. Махачкала, ул. Джержинского, 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