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

Информационная безопасность

Кафедра Информатики и информационных технологий

факультета Информатики и информационных технологий

Образовательная программа

09.03.03 Прикладная информатика
Профиль
Прикладная информатика в экономике
Прикладная информатика в менеджменте
Уровень высшего образования
бакалавриат

Форма обучения
Очная

Статус дисциплины: входит в обязательную часть ОПОП

Махачкала 2020

Рабочая программа дисциплины «Информационная безопасность» составлена в 2020 году в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.03 Прикладная информатика

от «12» марта 2015 г. № 207

Разработчик: каф. информатики и информационных технологий Гаджиев А.М., кандидат физ. – мат. наук, доцент.

Рабочая программа дисциплины одобрена:

на заседании кафедры информатики и информационных технологий

от « 12 » 03___2020г. протокол № 8

Зав. кафедрой _____ Ахмедов С.А.

(подпись)

На заседании Методической комиссии факультета Информатики и информационных технологий от

« 13 » 03__2020 г., протокол № 8

Председатель _____ Ахмедова З.Х.

(подпись)

Рабочая программа дисциплины согласована с учебно-методическим управлением

« 20 » 03 2020 г. _____

(подпись)

Аннотация рабочей программы дисциплины

Дисциплина «Информационная безопасность» входит в базовую часть образовательной программы *бакалавриата* по направлению 09.03.03 - Прикладная информатика

Дисциплина реализуется на факультете ИиИТ кафедрой информатики и информационных технологий.

Содержание дисциплины «Информационная безопасность» охватывает круг вопросов, связанных с ознакомлением студентов с основами информационной безопасности. Изучаются информационные угрозы, их нейтрализация, вопросы организации мер защиты информационных ресурсов, нормативные документы, регламентирующие информационную деятельность, криптография, другие вопросы, связанные с обеспечением безопасности компьютерных сетей.

Дисциплина нацелена на формирование следующих компетенций выпускника: общепрофессиональных - ОКП-3, ОКП-4.

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий в 4 семестре: лекции, практические занятия, самостоятельная работа.

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости в форме модульных контрольных работ и промежуточный контроль в форме зачета.

Объем дисциплины 3 зачетные единицы, 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						контроль	СРС, в том числе экзамен	
		всего	из них							
			Лекции	Лабораторные занятия	Практические занятия	КСР				
4	108	54	18		36			36	54	зачет

1. Цели освоения дисциплины

Целями освоения дисциплины (модуля) Информационная безопасность являются

- ознакомление студентов с основами информационной безопасности. Изучаются информационные угрозы, их нейтрализация, вопросы организации мер защиты информационных ресурсов, нормативные документы, регламентирующие информационную деятельность, другие вопросы, связанные с обеспечением безопасности компьютерных сетей.

- ознакомление с организационными, техническими, алгоритмическими и другими методами и средствами защиты компьютерной информации, с законодательством и стандартами в этой области, с современными криптосистемами, изучение методов идентификации пользователей, борьбы с вирусами, изучение методов защиты информации.

2.Место дисциплины в структуре ОПОП бакалавриата

Дисциплина «Информационные технологии» входит в базовую часть образовательной программы _бакалавриата по направлению (специальности) **09.03.03** Прикладная информатика.

Курс «Информационные безопасность» предусмотрен Федеральным государственным общеобразовательным стандартом высшего образования РФ и предназначен для бакалавров, обучающихся по направлению **09.03.03** «Прикладная информатика». Дисциплина «Информационные безопасность» относится к блоку Математических и естественнонаучных дисциплин, базовой части. Общая трудоемкость курса 108 часа, в том числе аудиторных занятий – 54 часа. Аудиторные занятия включают в себя лекции, практические занятия. Самостоятельная работа (54 часа) студентов состоит в самостоятельном изучении отдельных тем по учебной программе. Практические занятия, а также самостоятельная работа оцениваются и комментируются по мере выполнения. Чтение курса планируется в 4 семестре.

При освоении дисциплины студенты должны располагать знаниями приобретенные в результате освоения дисциплин «Информатика и программирование», «Информационные системы и технологии», «Проектирование е информационных систем», «Объектно-ориентированное программирование», «Операционные системы»

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

Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции	Результаты обучения
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Знает современные подходы к построению систем защиты информации
	ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Умеет выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации
	ОПК-3.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно- исследовательской работе с учетом требований информационной безопасности.	Владеть навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем
ОПК-4. Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.1. Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	Знает особенности обеспечения информационной безопасности компьютерных систем при обработке информации, составляющей государственную тайну
	ОПК-4.2. Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	Умеет пользоваться современной научно-технической информацией по исследуемым проблемам и задачам
	ОПК-4.3. Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы.	Владеет навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем

4. Объем, структура и содержание дисциплины.

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

4.2. Структура дисциплины.

№ п/п	Раздел Дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				Лекции	Лабор.	Практические	Контроль	Самостоятельная работа	
Модуль 1. Основы информационной безопасности и защиты информации									
1	Введение в информационную безопасность и защиту информации	4	1	2		4		6	Проверка домашнего задания.
2	Нормативно-правовое обеспечение информационной безопасности	4	2	2		4		6	Проведение практических занятий
3	Стандарты и спецификации в области информационной безопасности	4	3	2		4		6	Контрольная работа, модуль
	Итого за модуль			6		12		18	36
Модуль 2. Программно-технические сервисы информационной безопасности									
4	Основные программно-технические средства защиты информации	4	4	2		4		6	Проверка домашнего задания.
5	Модели и методики безопасности	4	5	2		4		6	Проведение практических занятий
6	Управление доступом, протоколирование и Аудит Экранирование и анализ защищенности	4	6	2		4		6	Контрольная работа, модуль
	Итого за модуль			6		12		18	36
Модуль 3. Основы криптографии и защита информации в ИС									
7	Основы криптографии	4	7	2		4		6	Проверка домашнего задания.
	Средства защиты информации в автоматизированных системах			2		4		6	Проведение практических занятий
8	Методология построения защищенных автоматизированных информационных	4	8	2		4		6	Контрольная работа, модуль

	систем								
	Итого за модуль			6		12		18	36
	Итого			**18**		**36**		**54**	**108**

4.2.1.1. Лекционный курс

№ п/п	Наименование темы	Трудоемкость	Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Технологии обучения
Модуль 1. Основы информационной безопасности и защиты информации						
	Введение в информационную безопасность и защиту информации	2	Назначение, задачи и общая характеристика курса, общие понятия и определения, краткая историческая справка. Данные и информация. Свойства информации. Машинное представление информации.	ОПК-3	Знает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности связанных с информационной безопасностью Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности. связанных с информационной безопасностью Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности, связанных с информационной безопасностью	модульное,проблемное, практико ориентированное
	Нормативно-правовое обеспечение информационной безопасности	2	Место информационной безопасности в национальной безопасности страны. Обзор законодательных актов.			
	Стандарты и спецификации в области информационной безопасности	2	Оценочные стандарты и технические спецификации. "Оранжевая книга" как оценочный стандарт Информационная безопасность распределенных систем.			
Модуль 2. Программно-технические сервисы информационной безопасности						

	Основные программно технические средства защиты информации	2	Основные понятия программно-технического уровня информационной безопасности Устройства и системы противоправного преднамеренного овладения конфиденциальной информацией.	ОПК-3,4	Умеет применять методы поиска и хранения информации с использованием современных информационных технологий. Знает теоретические основы поиска, хранения, и анализа Владеет навыками поиска, хранения и анализа информации с использованием современных информационных технологий.	модульное,проблемное, практико ориентированное
	Модели и методики безопасности	2	Модели безопасности и их применение. Модель матрицы доступа: добровольное и принудительное управление доступом. Модель распространения прав доступа.			
	Управление доступом, протоколирование и Аудит Экранирование и анализ защищенности	2	Логическое управление доступом Модели безопасности Ролевое управление доступом Возможный подход к управлению доступом в распределенной объектной среде			
Модуль 3. Основы криптографии и защита информации в ИС						
	Основы криптографии	2	Основные понятия. Классификация шифров. 2. Симметричное и асимметричное шифрование, поточное и блочное шифрование.	ОПК-4	Знает основы математики, физики, вычислительной техники и программирования. Умеет решать стандартные профессиональные задачи с применением естественнонаучных и общеинженерных знаний, методов математического анализа и моделирования. Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности, связанной с защитой информации и информационной безопасностью	модульное,проблемное, практико ориентированное
	Средства защиты информации в автоматизированных системах	2	Классификация систем. Основные средства защиты информации: технические, программные, криптографические, организационные, законодательные.			
	Методология построения защищенных автоматизированных информационных	2	Разработка решений по управлению предприятием. Внешнее отображение информации в системе. 3 типа данных, анализ которых позволяет производить прогнозирование			

4.2.1.2. Практические занятия

№ п/п	Наименование темы	Трудоемкость	Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Технологии обучения
Модуль 1. Основы информационной безопасности и защиты информации						
	Введение в информационную безопасность и защиту информации	2	Физическое представление информации и процессы ее обработки. Виды и формы представления информации. Носители информации. Информация как объект защиты.	ОПК-3	Знает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности. Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности. Имеет навыки применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.	модульное,проблемное, практико ориентированное
	Нормативно-правовое обеспечение информационной безопасности	2	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.			
	Стандарты и спецификации в области информационной безопасности	2	. Рекомендации X.800 Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий" Гармонизированные критерии Европейских стран			
Модуль 2. Программно-технические сервисы информационной безопасности						
	Основные программно технические средства защиты информации	2	Технические средства защиты объектов. Системы охранной сигнализации на территории и в помещениях объекта обработки информации. Требования к системам охранной сигнализации.	ОПК-3,4	Знает особенности обеспечения информационной безопасности компьютерных систем при обработке информации, составляющей государственную тайну Умеет пользоваться современной научно-технической информацией по исследуемым проблемам и задачам Владеет навыками	модульное,проблемное, практико ориентированное
	Модели и методики безопасности	2	Модель многоуровневой защиты данных. Модель безопасности информационных потоков. Управление рисками. Методики оценки рисков. Модель качественной оценки.			

			Количественная модель рисков.		формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем	
	Управление доступом, протоколирование и Аудит Экранирование и анализ защищенности	2	Понятия протоколирования и аудита Основные понятия экранирования Архитектурные аспекты экранирования			
Модуль 3. Основы криптографии и защита информации в ИС						
	Основы криптографии	2	Практическая стойкость шифров. ГОСТ 28147-89. Хэш-функции. Протоколы и алгоритмы шифрования. Криптосистемы. Системы управления ключами.	ОПК-4	Знает особенности обеспечения информационной безопасности компьютерных систем при обработке информации, составляющей государственную тайну Умеет пользоваться современной научно-технической информацией по исследуемым проблемам и задачам Владеет навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем	модульное,проблемное, практико ориентированное
	Средства защиты информации в автоматизированных системах	2	Средства контроля физического доступа. Автоматизированные средства защиты информации. Системы управления политикой безопасности. Работа с персоналом и оборудованием.			
	Методология построения защищенных автоматизированных информационных	2	Многомерная модель данных. Операции с измерениями			

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

4.3.1. Содержание лекционных занятий по дисциплине

1. Основы информационной безопасности и защиты информации

Тема 1 Введение в информационную безопасность и защиту информации

1. Назначение, задачи и общая характеристика курса, общие понятия и определения, краткая историческая справка.

2. Данные и информация. Свойства информации. Машинное представление информации. Физическое представление информации и

процессы ее обработки. Виды и формы представления информации. Носители информации. Информация как объект защиты.

3. Определение и цели, механизмы, инструментарий, основные направления информационной безопасности.

4. Информация и ресурсы. Информация как объект права собственности. Информация как коммерческая тайна. Информация как рыночный продукт.

Тема 2 Нормативно-правовое обеспечение информационной безопасности

1. Место информационной безопасности в национальной безопасности страны.

2. Обзор законодательных актов. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.

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

4. Закон Российской Федерации «О государственной тайне». Федеральный закон Российской Федерации «Об информации, информационных технологиях и защите информации». Федеральный закон Российской Федерации «Об электронной цифровой подписи».

5. Стандарты предприятия.

Тема 3. Стандарты и спецификации в области информационной безопасности

1. Оценочные стандарты и технические спецификации. "Оранжевая книга" как оценочный стандарт

2. Информационная безопасность распределенных систем. Рекомендации X.800

3. Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий"

4. Гармонизированные критерии Европейских стран

5. Интерпретация "Оранжевой книги" для сетевых конфигураций

6. Руководящие документы Гостехкомиссии России

Модуль 2. Программно-технические сервисы информационной безопасности

Тема 4 Программно-технические средства защиты информации

1. Основные понятия программно-технического уровня информационной безопасности

2. Устройства и системы противоправного преднамеренного овладения конфиденциальной информацией. Технические средства защиты объектов. Системы охранной сигнализации на территории и в помещениях объекта обработки информации. Требования к системам охранной сигнализации.

3. Защита информации от утечки за счет побочного электромагнитного излучения и наводок.Методы и средства защиты

информации от случайных воздействий. Методы защиты информации от аварийных ситуаций. Биометрия, интеллектуальные карты.

4. Особенности современных информационных систем, существенные с точки зрения безопасности

5. Архитектурная безопасность

Тема 5 Модели и методики безопасности

1. Модели безопасности и их применение.

2. Модель матрицы доступа: добровольное и принудительное управление доступом.

3. Модель распространения прав доступа.

4. Модель многоуровневой защиты данных. Модель безопасности информационных потоков.

5. Управление рисками. Методики оценки рисков. Модель качественной оценки. Количественная модель рисков.

6. Определение вероятности события. Определение стоимости активов.

7. Использование списков уязвимостей в управлении рисками.

Тема 6.Управление доступом, протоколирование и аудит

1. Логическое управление доступом

2. Модели безопасности

3. Ролевое управление доступом

4. Возможный подход к управлению доступом в распределенной объектной среде

5. Понятия протоколирования и аудита

6. Активный аудит

Тема 13. Экранирование и анализ защищенности

1. Основные понятия экранирования

2. Архитектурные аспекты экранирования

3. Классификация межсетевых экранов

4. Анализ защищенности

Модуль 3. Основы криптографии и защита информации в ИС

Тема 7. Основы криптографии

1. Основные понятия. Классификация шифров.

2. Симметричное и асимметричное шифрование, поточное и блочное шифрование. Практическая стойкость шифров.

3. ГОСТ 28147-89.

4. Хэш-функции. Протоколы и алгоритмы шифрования. Криптосистемы.

5. Системы управления ключами.

6. Электронная цифровая подпись. ГОСТ Р 34.10-2001

Тема 8. Средства защиты информации в автоматизированных системах

1. Классификация систем.

2. Основные средства защиты информации: технические, программные, криптографические, организационные, законодательные. Средства контроля физического доступа.

3. Автоматизированные средства защиты информации. Системы управления политикой безопасности. Работа с персоналом и оборудованием.

4. Автоматизированные системы как объекты защиты информации.

5. Организация проектирования автоматизированных систем в защищенном исполнении.

6. Условия и режимы эксплуатации автоматизированных систем.

Тема 9. Методология построения защищенных автоматизированных информационных систем

1. Критерии защищенности. Анализ и оценка действующей концепции защиты.

2. Выбор концептуальной модели построения защиты. Исходные данные для постановки задачи.

3. Введение в проблему теории защиты информации. Общий методический подход.

4. Модель элементарной защиты. Модель многозвенной защиты. Многоуровневая защита.

5. Метод построения защиты информации в системах с сосредоточенной обработкой данных.

6. Классификация возможных каналов НСД.

4.3.2. Содержание практических занятий по дисциплине

5. Образовательные технологии

Рекомендуемые образовательные технологии: лекции, лабораторные и практические занятия, самостоятельная работа бакалавров.

В соответствии с требованиями ФГОС ВПО по направлению подготовки реализация компетентностного подхода предусматривает широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, разбор конкретных ситуаций) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся. В рамках учебных курсов предусмотрены встречи с представителями российских и зарубежных компаний, государственных и общественных организаций, мастер-классы экспертов и специалистов.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью (миссией) программы, особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом в учебном процессе они должны составлять не менее 30% аудиторных занятий (определяется требованиями ФГОС с учетом специфики ООП). Занятия лекционного типа для соответствующих групп студентов не могут

составлять более 60% аудиторных занятий (определяется соответствующим ФГОС)).

Вид занятия	Технология	Цель	Формы и методы обучения
1	2	3	4
Лекции	Технология проблемного обучения	Усвоение теоретических знаний, развитие мышления, формирование профессионального интереса к будущей деятельности	Мультимедийные лекция-объяснение, лекция-визуализация, с привлечением формы тематической дискуссии, беседы, анализа конкретных ситуаций
Практические занятия	Технология проблемного, модульного, дифференцированного и активного обучения, деловой игры	Развитие творческой и познавательной самостоятельности, обеспечение индивидуального подхода с учетом базовой подготовки. Организация активности студентов, обеспечение личностно деятельного характера усвоения знаний, приобретения навыков, умений.	Индивидуальный темп обучения. Постановка проблемных познавательных задач. Методы активного обучения: «круглый стол», игровое производственное проектирование, анализ конкретных ситуаций.
Самостоятельная работа	Технологии концентрированного, модульного, дифференцированного обучения	Развитие познавательной самостоятельности, обеспечение гибкости обучения, развитие навыков работы с различными источниками информации, развитие умений, творческих	Индивидуальные, групповые, интерактивные (в режимах on-line и off-line).

6.Учебно-методическое обеспечение самостоятельной работы студентов.

Методические рекомендации студентам по организации самостоятельной работы при изучении дисциплины «Информационные технологии»

При подготовке к коллоквиуму, экзамену каждый студент должен индивидуально готовиться по темам дисциплины, читая конспекты лекций и рекомендуемую учебную и справочную литературу, усваивая определения, схемы и принципы соответствующих расчетов. Самостоятельная работа позволяет студенту в спокойной обстановке подумать и разобраться с информацией по теме, структурировать знания. Чтобы содержательная информация по дисциплине запоминалась надолго, целесообразно изучать ее поэтапно, в предлагаемой последовательности, поскольку последующий материал связан с предыдущим. По каждой из тем для самостоятельного изучения, приведенных в рабочей программе дисциплины следует сначала прочитать рекомендованную литературу и при необходимости составить краткий конспект основных положений, терминов, сведений, требующих запоминания и являющихся основополагающими в этой теме и для освоения последующих разделов курса.

При выполнении индивидуальных заданий студент использует приобретенные на практических занятиях навыки расчетов, самостоятельно изучает примеры из лекций, электронно-образовательных ресурсов размещенных на сайте ДГУ и соответствующего раздела дисциплины. Самостоятельная работа при выполнении индивидуальных заданий требует изучения и использования справочных материалов. Залогом успеха в приобретении знаний и навыков по дисциплине является синхронизация выполняемых индивидуальных заданий по срокам с лекционным материалом и разбираемым на практических занятиях.

Методические рекомендации по самостоятельной подготовке к лабораторным занятиям (контрольные вопросы)

2. Законодательство в области информационной безопасности
3. Криптографические методы и средства защиты информации в компьютерных системах и сетях
4. Политика и модели безопасности
5. Безопасность сетевых операционных систем
6. Безопасность локальных и глобальных сетевых технологий
7. Радиоэлектронные системы и устройства защиты информации
8. Комплексная защита информации в компьютерных системах и сетях Актуальность проблем информационной безопасности в современном мире.
9. Задачи и методы обеспечения информационной безопасности в сфере внешней и внутренней политики России.
10. Информация - наиболее ценный ресурс современного общества.
11. Проблемы информационных войн на современном этапе.
12. Государственная информационная политика РФ.
13. Государственная система правового обеспечения защиты информации в РФ.

14. Государственное регулирование использования криптографических средств.
15. Государственное регулирование использования электронной цифровой подписи.
16. Информационнаябезопасность в государственной информационной политике РФ.
17. Информация как объект юридической защиты.
18. Информационное право на современном этапе развития общества.
19. Задачи и принципы организации службы информационной безопасности предприятий.
20. Зарубежное законодательство в области информационной безопасности.
21. Зарубежные стандарты в области информационной безопасности.
22. Информационнаябезопасность беспроводных сетей.
23. Информационная безопасность компьютерных сетей.
24. Современное информационное оружие и его классификация.
25. Информация как наиболее ценный ресурс современного общества.
26. Категории информации по режиму ограничения доступа и использования.
27. Лицензирование, сертификация и аттестация объектов информатизации и защиты информации.
28. Использование криптографических и стеганографических методов в информационном обмене.
29. Международные стандарты информационного обмена.
30. Обеспечение информационной безопасности в Internet.
31. Основные положения Доктрины информационной безопасности.
32. Отечественные стандарты в области информационной безопасности.
33. Оценка безопасности информационных технологий.
34. Организационная структура государственной системы обеспечения информационной безопасности РФ.
35. Базовые источники системы информационной безопасности.
36. Правонарушения и ответственность в области эксплуатации информационных систем и информационной безопасности.
37. Правовая основа системы информационной безопасности.
38. Нормативно-правовое обеспечение в сфере связи и коммуникаций.
39. Корпоративная политика информационной безопасности.
40. Проблемы информационной безопасности в национальном и международном аспектах.
41. Проблемы информационной безопасности в области государственного и муниципального управления.
42. Программно-технический уровень информационной безопасности.
43. Современное состояние нормативно-правовой базы информационной безопасности.
44. Система подготовки кадров в области информационной безопасности в РФ.

45. Угрозы безопасности информации и информационные атаки.
46. Угрозы информационной безопасности в компьютерных сетях.
47. Управление информационными рисками.
48. Электронная цифровая подпись - правовой и технический аспекты.

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.

Компетенция	Планируемые результаты обучения	Процедура освоения
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знает**: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. **Умеет**: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности. **Владеет**: . Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	Устный опрос, выступление на практических занятиях контрольная работа
ОПК-4. Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	**Знает**: основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. **Умеет**: применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы. **Владеет**: навыками составления технической документации на различных этапах жизненного цикла информационной системы.	Устный опрос, выступление на практических занятиях контрольная работа

7.2. Типовые контрольные тесы

1. Троянские программы. Алгоритмы работы.
2. "Черви", методика внедрения. Примеры.

3. Настройки защиты электронной почты.
4. Технические методы защиты.
5. Косвенные каналы утечки информации и методики противодействия.
6. Защита от сетевых атак.
7. Уязвимости современных операционных систем. Методы устранения уязвимостей.
8. Анализ недостатков информационной безопасности Российской Федерации.
9. Методика построения защищенного рабочего места с выходом в глобальную сеть.
10. Модели доступа к данным (Биба, сазерлендская и т.д.).
11. Виды программ-закладок. Методика противодействия.
12. Типовые удаленные атаки с использованием уязвимостей сетевых протоколов. Классификация удаленных атак.
13. Модели защиты информации в КС
14. Руководящие документы Гостехкомиссии России. ГОСТы в области информационной безопасности.
15. Реализация дискреционной модели в операционных системах семейства Windows.
16. Методики оценки защищенности операционных систем.
17. Методики защиты информации, составляющей государственную тайну.
18. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
19. Виды программ-закладок. Методика противодействия.
20. Эмуляторы и создание образов дисков. Методы противодействия.
21. Важность законодательного уровня информационной безопасности
22. Обзор российского законодательства в области информационной безопасности
23. Закон "Об информации, информатизации и защите информации"
24. О текущем состоянии российского законодательства в области информационной безопасности
25. Обзор зарубежного законодательства в области информационной безопасности
26. Классы безопасности в интерпретации «Оранжевой книги»

Примерный перечень вопросов к зачету

1. Понятие информационной безопасности.
2. Основные составляющие информационной безопасности.
3. Важность и сложность проблемы информационной безопасности
4. Основные определения и критерии классификации угроз.
5. Наиболее распространенные угрозы.
6. Вредоносное программное обеспечение.
7. Основные понятия управления рисками и их основные этапы

8. Понятие «Законодательный уровень информационной безопасности» и его важность.
9. Понятие административного уровня обеспечения информационной безопасности.
10. Процедурный уровень информационной безопасности
11. Оценочные стандарты и технические спецификации. "Оранжевая книга" как оценочный стандарт.
12. Информационная безопасность распределенных систем.
13. Рекомендации X.800.
14. Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий".
15. Руководящие документы Гостехкомиссии России
16. Основные понятия программно-технического уровня информационной безопасности.
17. Особенности современных информационных систем, существенные с точки зрения безопасности.
18. Архитектурная безопасность
19. Понятие идентификации и аутентификации.
20. Парольная аутентификация.
21. Идентификация/аутентификация с помощью биометрических данных.
22. Управление доступом основные понятия
23. Понятие протоколирования и аудита, активный аудит.
24. Функциональные компоненты и архитектура.
25. Основы криптографии, шифрование и виды шифров.
26. Контроль целостности, алгоритмы шифрования
27. 27. Основные понятия экранирования и анализ защищенности.
28. Архитектурные аспекты экранирования.
29. Классификация межсетевых экранов.
30. Анализ защищенности

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

Программой дисциплины в целях проверки прочности усвоения материала предусматривается проведение различных форм контроля:

1. «Входной» контроль определяет степень сформированности знаний, умений и навыков обучающегося, необходимым для освоения дисциплины и приобретенным в результате освоения предшествующих дисциплин.

2. Тематический контроль определяет степень усвоения обучающимися каждого раздела (темы в целом), их способности связать учебный материал с уже усвоенными знаниями, проследить развитие, усложнение явлений, понятий, основных идей.

3. Межсессионная аттестация – рейтинговый контроль знаний студентов, проводимый в середине семестра.

4. Рубежной формой контроля является экзамен. Изучение дисциплины завершается зачетом, проводимым в виде письменного опроса с учетом текущего рейтинга.

Рейтинговая оценка знаний студентов проводится по следующим критериям:

Вид оцениваемой учебной работы студента	Баллы за единицу работы	Максимальное значение
Посещение всех лекции	макс. 5 баллов	5
Присутствие на всех практических занятиях	макс. 5 баллов	5
Оценивание работы на семинарских, практических, лабораторных занятиях	макс. 10 баллов	10
Самостоятельная работа	макс. 40 баллов	40
Итого		60

Неявка студента на промежуточный контроль в установленный срок без уважительной причины оценивается нулевым баллом. Повторная сдача в течение семестра не разрешается.
Дополнительные дни отчетности для студентов, пропустивших контрольную работу по уважительной причине, подтвержденной документально, устанавливаются преподавателем дополнительно.
Лабораторные работы, пропущенные без уважительной причины, должны быть отработаны до следующей контрольной точки, если сдаются позже, то оцениваются в 1 балл.
Студенты, набравшие от 51 до 100 баллов, получают зачет по дисциплине без проведения дополнительных испытаний, если сумма набранных баллов меньше 50, то студент пишет итоговый тест по дисциплине в последнюю учебную неделю семестра.

Итоговой формой контроля знаний, умений и навыков по дисциплине является **(зачет)**. Зачет проводится по тестам или по билетам, которые включают 2 (два) теоретических вопроса.

Экзамен проводится по тестам или по билетам, которые включают 2 (два) вопроса теоретический, практический.

Оценка знаний студентов производится по следующим критериям:

– знание на хорошем уровне содержания вопроса;

- знание на хорошем уровне терминологии компьютерной графики;
- знание на хорошем уровне перспектив и направлений развития компьютерной графики;
- использование в ответе материала из дополнительной литературы;
- умение привести практический пример использования конкретных приемов и методов компьютерной графики;
- использование в ответе самостоятельно найденных примеров;
- наличие собственной точки зрения по проблеме и умение ее защитить;
- знание на хорошем уровне методов, алгоритмов и технологий построения, функционирования и использования компьютерной графики;
- умение четко, кратко и логически связно изложить материал.

При соответствии ответа учащегося на зачете более чем 50 % критериев из этого списка выставляется оценка «зачет», в случае несоответствия – «незачет».

Вторым вариантом проведения зачета является проверка знаний учащихся с помощью с помощью электронных тестов, в этом случае оценка «зачет» ставится при правильном ответе как минимум на 60 % предложенных вопросов.

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.ЫЫюdub.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.

Студенты очной формы обучения нормативного срока обучения изучают дисциплину "Информационные технологии" в течение 3-4 семестров. Виды и объем учебных занятий, формы контроля знаний приведены в табл. 1. Темы и разделы рабочей программы, количество лекционных часов и количество часов самостоятельной работы студентов на каждую из тем приведены в табл. 2. В первой колонке этой таблицы указаны номера тем согласно разделу 4. Организация лабораторного практикума, порядок подготовки к лабораторным занятиям и методические указания к самостоятельной работе студентов, а также порядок допуска к лабораторным занятиям и отчетности по проделанным работам определены в методических указаниях по выполнению лабораторных работ.

Самостоятельная работа студентов в ходе изучения лекционного материала заключается в проработке каждой темы в соответствии с методическими указаниями, а также в подготовке выполнения лабораторных работ, которые выдаются преподавателем на лекционных занятиях.

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

Технические средства

- Проектор;

а) Мультимедийная аудитория - для лекций;

Для проведения лекционных занятий требуется аудитория на курс, оборудованная интерактивной доской, мультимедийным проектором с экраном.