МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет математики и компьютерных наук

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопастность и защита информации

Кафедра дискретной математики
факультет математики и компьютерных наук

Образовательная программа

01.03.02 Прикладная математика и информатика

Профиль подготовки
Математическое моделирование и вычислительная математика

Уровень высшего образования
бакалавриат

Форма обучения
очная

Статус дисциплины: **вариативная по выбору**

Махачкала - 2017

Рабочая программа дисциплины «Информационная безопасность и защита информации» составлена в 2017 году в соответствии с требованиями ФГОС ВО по направлению подготовки

01.03.02 - Прикладная математика и информатика (уровень бакалавриат)

Приказ Минобрнауки России от 12.03.2015 №228

Разработчик: кафедра дискретной математики,
Ибрагимов Мурад Гаджиевич, к. ф.-м. н., доцент.

Рабочая программа дисциплины «Информационная безопасность и защита информации» одобрена:
на заседании кафедры дискретной математики от «13» 01 2017 г., протокол № 5
Зав. кафедрой _____ Магомедов А.М.

на заседании Методической комиссии факультета математики и компьютерных наук от «17» 01 2017 г., протокол № 5
Председатель _____ Меджидов З.Г.

Рабочая программа дисциплины согласована с учебно-методическим управлением «____» _____ 20___ г. _____

Содержание

Аннотация рабочей программы дисциплины

Аннотация рабочей программы дисциплины

Дисциплина **«Информационная безопасность и защита информации»** входит в вариативную часть образовательной программы **бакалавриата** по направлению **01.03.02-Прикладная математика и информатика** и является дисциплиной по выбору.

Дисциплина реализуется на факультете математики и компьютерных наук кафедрой дискретной математики.

Принципы отбора содержания и организации учебного материала Дисциплина «Информационная безопасность и защита информации» призвана содействовать знакомству студентов с компьютерными телекоммуникациями и возможными подходами к разработке гипертекстовых документов, предназначенных для публикации в глобальной компьютерной сети Internet. Она важна с той точки зрения, что позволяет развивать способности студентов, связанные с общей культурой работы в глобальной сети. Общая проблема информационной безопасности информационных систем; защита информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение); организационное обеспечение информационной безопасности; защита информации от несанкционированного доступа; математические и методические средства защиты; компьютерные средства реализации защиты в информационных системах; программа информационной безопасности России и пути ее реализации.

Для полноценного усвоения учебного материала по дисциплине "Информационная безопасность и защита информации" студентам необходимо иметь прочные знания по технологии программирования, теории вычислительных сетей, информационным технологиям. Курс закрепляет навыки работы с текстом и графикой, а также навыков программирования и проектирования и разработки информационных систем, являясь, таким образом, прямым продолжением курсов «Информатика и программирование», «Информационные технологии», «Объектно-ориентированное программирование», «Базы данных», «Информационные системы», «Проектирование информационных систем» и многих других.

Рабочая программа дисциплины способствует решению следующих типовых задач учебно-профессиональной деятельности: осуществление процесса обучения принципам построения и эффективного применения информационных систем, операционных оболочек, обслуживающих сервисных программ в соответствии с образовательной программой; организация самостоятельной работы и внеурочной деятельности студентов.

Дисциплина нацелена на формирование следующих компетенций выпускника:
общепрофессиональных – **ОПК-2, ОПК-4**.
профессиональных – **ПК-5, ПК-7**.

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

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости в форме **контрольной работы, коллоквиума и тестирования**.
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							
	Контактная работа обучающихся с преподавателем						СРС, в том числе экзамен	
	Всего	из них						
		Лекции	Лабораторные занятия	Практические занятия	КСР	консультации		
8	108	16	16	16	-	-	60	зачет

1. Цели освоения дисциплины

Цель изучения дисциплины состоит в формировании системного базового представления, умения и навыков студентов по основам информационной безопасности и защите информации, достаточных для последующей эксплуатации автоматизированных систем (АС) и сетей отраслей. Основными целями преподавания дисциплины являются:

- изучение методов построения технических средств защиты объектов и информации;
- изучение методов защиты автоматизированных систем обработки данных от несанкционированного доступа к информации;
- изучение математических и методических средств защиты;
- изучение законодательных мер по защите информации.

Целью курса является освоение практических приемов информационной безопасность и защиты информации. В лекционной части курса рассматриваются общие принципы информационной безопасности и защиты информации. Изучение всех тем сопровождается иллюстрирующими примерами. Лабораторные работы в компьютерных классах служат для индивидуальной работы студентов над учебными задачами и итоговым проектом с целью выработки и закрепления практических навыков информационной безопасности и защиты информации.

Задачи курса - овладение теоретическими, практическими и методическими вопросами обеспечения информационной безопасности и освоение системных комплексных методов защиты предпринимательской информации от различных видов объективных и субъективных угроз в процессе ее возникновения, обработки, использования и хранения. Изучаемые вопросы рассматриваются в широком диапазоне современных проблем и затрагивают предметные сферы защиты как документированной информации

(на бумажных и технических носителях), циркулирующей в традиционном или электронном документообороте, находящейся в компьютерных системах, так и недокументированной информации, распространяемой персоналом в процессе управленческой (деловой) или производственной деятельности.

Перечень дисциплин и тем, усвоение которых студентами необходимо для изучения данной дисциплины. Для полноценного усвоения учебного материала по дисциплине "Информационная безопасность и защита информации" студентам необходимо иметь прочные знания по технологии программирования, теории вычислительных сетей, информационным технологиям, нормы государственного стандарта, общая проблема информационной безопасности информационных систем; защита информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение); организационное обеспечение информационной безопасности; защита информации от несанкционированного доступа; математические и методические средства защиты; компьютерные средства реализации защиты в информационных системах; программа информационной безопасности России и пути ее реализации.

Основные задачи курса. В процессе обучения студенты должны изучить правовую базу информационной безопасности информационных систем, угрозы информационной безопасности корпоративных систем отраслей, методы защиты информации, включая криптографические, способы защиты информации от несанкционированного доступа к информации и техническим ресурсам корпоративных сетей отраслей, архитектуру и методы организации систем защиты информации. Это достигается с помощью лекций и выполнения лабораторных работ, а также самоподготовки студентов.

2.Место дисциплины в структуре ООП бакалавриата

Дисциплина «Информационная безопасность и защита информации» входит в вариативную часть и является дисциплиной по выбору образовательной программы бакалавриата, по направлению 01.03.02 - Прикладная математика и информатика.

Ядро курса составляют темы, посвященные концепции национальной безопасности и доктрине информационной безопасности, комплексу межотраслевых законодательных актов в сфере правовой защиты информации, формированию и использованию государственной тайны и системе тайн, касающихся информации ограниченного доступа; сущности конфиденциального делопроизводства. Изучение означенных тем является обязательным. Особого внимания заслуживает тема государственной тайны, предусматривающая наиболее серьезную уголовную ответственность, а также темы коммерческой тайны и интеллектуальной собственности, как наиболее актуальные в рыночных условиях. Тема доктрины информационной безопасности важна не только тем, что раскрывает сущность данного вопроса, но и показывает взгляд государства на состояние и обеспечение информационной безопасности государства, общества и граждан. Не меньшее

внимание следует уделить в рыночных условиях теме организации защищенного документооборота, когда конфиденциальная информация становится конкурентным преимуществом на рынке.

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

Компетенции	Формулировка компетенции из ФГОС ВО	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)
ОПК-2	Способностью приобретать новые научные и профессиональные знания, используя современные образовательные и информационные технологии	**Знать**: детально методы и базовые алгоритмы обработки информационных структур, методов получения новой информации; **Уметь**: использовать свои знания на практике; **Владеть**: основными методами, способами и средствами получения, хранения, переработки информации, иметь навыки работы с компьютером как средством управления информацией; пониманием концепций, синтаксической и семантической организации, методов использования современных языков программирования; пониманием концепций, базовых алгоритмов, принципов разработки и функционирования современных операционных систем.
ОПК-4	Способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знать:** - правовую и нормативную базу корпоративных информационных систем отраслей; - информационную структуру и информационные ресурсы сетей отраслей как объекта защиты; - основные устройства и системы защиты объектов и информации; - основные типы методов, устройств и систем технической разведки; - методы защиты автоматизированных систем обработки данных от несанкционированного доступа к информации, в том числе: специальные технические средства опознавания пользователя ПЭВМ; - специальное программное обеспечение по защите информации ПЭВМ; - основные типы методов, устройств и систем технической разведки; специальные средства защиты от несанкционированного доступа; - организацию вычислительных работ, уменьшающую риск потери информации; - сущность, цели и принципы экономической безопасности предпринимательской деятельности, направления их практической реализации; концепцию

		информационной безопасности, конституционные и законодательные основы ее реализации. **Уметь**: - создавать простейшие статические web-документы в графическом многооконном режиме, так и в режиме командной строки (консоли); - применять современные системные программные средства, технологии и инструментальные средства; - применять язык C# для разработки динамических страниц сети Internet; - размещать сценарии PHP на HTML-странице; - работать в среде пакета Microsoft Visual Studio; - работать в среде пакета MSSQL Server; - использовать графические программы для создания чертежей структуры web-сайта; - использовать графические редакторы для обработки изображений, размещаемых на web-сайте. **Владеть**: - навыками работы с межсетевыми экранами и пакетами антивирусных программ; - навыками самостоятельного проектирования систем защиты информации с техническими средствами разведки, защиты информации и противодействия коммерческой разведке; - навыками работы с межсетевыми экранами и пакетами антивирусных программ; - навыками самостоятельного проектирования систем защиты информации; - с техническими средствами разведки, защиты информации и противодействия коммерческой разведке.
ПК-5	Способностью осуществлять целенаправленный поиск информации о новейших научных и технологических достижениях в информационно-телекомуникационной сети «Интернет» и других источниках	**Знать**: основные принципы работы в информационно-телекомуникационной сети Internet. **Уметь**: применять полученные знания для поиска информации о новейших научных и технологических достижениях в информационно-телекомуникационной сети Internet и других источниках. **Владеть**: навыками безопасной работы в сети Internet.
ПК-7	Способностью к разработке и применению алгоритмических и программных решений в области системного и прикладного программного обеспечения	**Знать**: методы и приемы разработки и применения алгоритмических и программных решений в области системного и прикладного программного обеспечения. **Уметь**: - применять современные системные программные средства, технологии и инструментальные средства; - работать в среде пакета Microsoft.

		Владеть: - навыками работы в системе Windows; - навыками разработки статических и динамических страниц сети Internet; - навыками программирования на языке PHP.

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	Неделя семестра	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 занятия	Лаб. занят.	Контроль самост. раб.		
1	**Модуль 1**								
2	**Тема 1.** Предмет, цели и задачи дисциплины «Информационная безопасность и защита информации». Основные определения и понятия. Законодательство в области информационной безопасности и защиты данных. Структуры и нормативные акты, их направления.	8	1	2	2	2		8	Устный опрос, письменная контрольная работа, лабораторная работа.
3	**Тема 2.** Классификация информационных ресурсов, характеристика и основные свойства. Информационные ресурсы в современных условиях, требования к ним, надежность (достоверность) информации и защиты от несанкционированного доступа. Классификация и анализ угроз информационной	8	2	2	2	2		8	

	безопасности корпоративным системам. Уровни защиты информации: правовой; организационный; аппаратно-программный; криптографический.								
4	**Тема 3.** Классификация криптографических методов. Традиционные (симметричные) криптосистемы. Блоковые и поточные шифры. Стойкость криптосистем. Американский стандарт шифрования данных DES. Отечественный стандарт криптографической защиты ГОСТ 28147-89. Асимметричные криптосистемы. Математические основы криптографии с открытым ключом. Криптосистема RSA. Криптосистема Эль Гамаля. Криптосистемы без передачи ключей. Управление ключами. Методы генерации, хранения и распределения ключей. Протоколы управления ключами.	8	3	2	2	2		8	
5	**Итого по модулю 1:**	**8**	**1-3**	**6**	**6**	**6**		**24**	Коллоквиум
6	**Модуль 2**								
7	**Тема 4.** Аппаратно-программные решения защиты информации в информационных системах. Электронные замки. Инфраструктура открытых ключей. Цифровые сертификаты. Электронная цифровая подпись (ЭЦП). Однонаправленная хэш-функция. Идентификация и аутентификация объектов	8	4	2	2	2		12	Устный опрос, письменная контрольная работа,

	сети. Идентификация и подтверждение подлинности пользователей сети.								лабораторная работа.
8	**Тема 5.** Математические методы обеспечения защиты от несанкционированного доступа и конфиденциальности. Криптография: понятия, подходы, направления исследований.	8	5	2	2	2		12	
9	**Итого по модулю 2:**	**8**	**4-5**	**4**	**4**	**4**		**24**	Коллоквиум
10	**Модуль 3**								
11	**Тема 6.** Межсетевое экранирование. Принципы построения и функционирования межсетевых экранов (МЭ). Классификация МЭ. Особенности межсетевого экранирования на различных уровнях модели OSI. Криптография и криптоанализ в авторизации, аутентификации и в обмене информации. Основные понятия и принципы криптографии. Особенности реализация криптографических методов.	8	6	2	2	2		8	Устный опрос, письменная контрольная работа, лабораторная работа.
12	**Тема 7.** Средства антивирусной защиты. Классификация вирусов и средств защиты. Виды антивирусных программных продуктов. Характеристика наиболее популярных антивирусных пакетов. Архитектура системы защиты информации (СЗИ). Этапы создания СЗИ. Виды обеспечения СЗИ. Принципы разработки СЗИ.	8	7	2	2	2		8	

13	**Тема 8.** Информационная безопасность в глобальном информационном пространстве Интернет. Безопасная интеграция в Интернет. Программные и технологические решения. Угрозы и риски интернет-технологий. Стандартизация информационной безопасности в Интернет. Программно-аппартные технологии Интернет. Основные понятия и принципы криптографии. Особенности реализация криптографических методов.	8	8	2	2	2		8	
14	**Итого по модулю 3:**	**8**	**6-8**	**6**	**6**	**6**		**24**	Коллоквиум
15	**Итого за 8 семестр:**	**8**	**1-8**	**16**	**16**	**16**		**60**	Зачет
16	**Итого:**	**8**	**1-8**	**16**	**16**	**16**		**60**	**Зачет**

4.3. Содержание дисциплины, структурированное по темам (разделам)

Модуль 1

Лекция 1. Предмет, цели и задачи дисциплины «Информационная безопасность и защита информации». Основные определения и понятия.

Законодательство в области информационной безопасности и защиты данных. Структуры и нормативные акты, их направления.

План-вопросы:

1. Классификация нормативных актов в области ИБ и ЗД;
2. Государственные органы, регулирующие вопросы информационной безопасности;
3. Классификация информации по степени ее защиты;
4. Доктрина информационной безопасности РФ;
5. Законодательство и нормативные акты Российской Федерации.

Лекция 2. Классификация информационных ресурсов, характеристика и основные свойства. Информационные ресурсы в современных условиях, требования к ним, надежность (достоверность) информации и защиты от несанкционированного доступа.

Классификация и анализ угроз информационной безопасности корпоративным системам. Уровни защиты информации: правовой; организационный; аппаратно-программный; криптографический.

Лекция 3. Классификация криптографических методов. Традиционные (симметричные) криптосистемы. Блоковые и поточные шифры. Стойкость криптосистем. Американский стандарт шифрования данных DES. Отечественный стандарт криптографической защиты ГОСТ 28147-89.

Асимметричные криптосистемы. Математические основы криптографии с открытым ключом. Криптосистема RSA. Криптосистема Эль Гамаля. Криптосистемы без передачи ключей. Управление ключами. Методы генерации, хранения и распределения ключей. Протоколы управления ключами.

Модуль 2

Лекция 4. Аппаратно-программные решения защиты информации в информационных системах.

План-вопросы:

1. Аппаратно-программные средства контроля доступа
1.1. iButton.
1.2 Смарт-карты.
1.3. Устройства ввода на базе USB-ключей.
1.4. Proximity.
1.5. Биометрические УВИП
1.6. Комбинированные устройства ввода.
2. Электронные замки.

Инфраструктура открытых ключей. Цифровые сертификаты. Электронная цифровая подпись (ЭЦП). Однонаправленная хэш-функция.

Идентификация и аутентификация объектов сети. Идентификация и подтверждение подлинности пользователей сети.

Лекция 5. Математические методы обеспечения защиты от несанкционированного доступа и конфиденциальности.

План-вопросы:

1. Исторический очерк развития криптографии
1.1. Криптография древнего периода.
1.2. Криптография арабского мира.
1.3. Криптография в эпоху Возрождения (XIV-XVI вв.).
1.4. Криптография в XVII-XVIII веках.
1.5. Криптография в XIX веке.
1.6. Криптография в XX веке.
1.7. О криптографии нового времени.
2. Криптография: понятия, подходы, направления исследований.
2.1 Предисловие.
2.2. Базовая терминология.
2.3. Основные алгоритмы шифрования.
2.4. Цифровые подписи.
2.5. Криптографические хэш-функции.
2.6. Криптографические генераторы случайных чисел.
2.7. Обеспечиваемая шифром степень защиты.

2.8. Криптоанализ и атаки на криптосистемы.

Модуль 3

Лекция 6. Межсетевое экранирование. Принципы построения и функционирования межсетевых экранов (МЭ). Классификация МЭ. Особенности межсетевого экранирования на различных уровнях модели OSI.

Криптография и криптоанализ в авторизации, аутентификации и в обмене информации.

План–вопросы:

1. Основные понятия и принципы криптографии.
1.1 Симметричные криптосистемы.
1.2 Асимметричные криптосистемы.
1.3 Электронная цифровая подпись.
1.4 Управление ключами в криптографических системах защиты информации.
2. Особенности реализация криптографических методов.
2.1 Федеральная инфраструктура открытых ключей.
2.2 Направления исследований в области криптосистем.

Лекция 7. Средства антивирусной защиты. Классификация вирусов и средств защиты. Виды антивирусных программных продуктов. Характеристика наиболее популярных антивирусных пакетов.

Архитектура системы защиты информации (СЗИ). Этапы создания СЗИ. Виды обеспечения СЗИ. Принципы разработки СЗИ.

Лекция 8. Информационная безопасность в глобальном информационном пространстве Интернет. Безопасная интеграция в Интернет. Программные и технологические решения.

План-вопросы:

1. Угрозы и риски интернет-технологий.
2. Стандартизация информационной безопасности в Интернет.
3. Программно-аппартные технологии Интернет.
3.1 Брандмауэры.
3.2 Программное обеспечение защиты информации в Интернет.
4 Основные понятия и принципы криптографии.
4.1 Симметричные криптосистемы.
4.2 Асимметричные криптосистемы.
4.3 Электронная цифровая подпись.
4.4 Управление ключами в криптографических системах защиты информации.
5. Особенности реализация криптографических методов.

Лабораторные работы (лабораторный практикум)

Лабораторные работы в компьютерных классах служат для самостоятельной работы студентов над учебными задачами с целью выработки и закрепления практических навыков по предмету «Информационная безопасность и защита информации».

Лабораторная работа	Цель и содержание лабораторной работы	Результаты лабораторной работы
Модуль1		
Лабораторная работа 1. Защита баз данных на примере MS ACCESS.	Алгоритм защиты БД MS Access. Порядок выполнения и результаты работы.	Защита на уровне пароля. Защита на уровне пользователя. Создать и изменить пароль.
Лабораторная работа 2. Стандартные способы зашиты информации.	О сложности паролей. Защита информации в офисных документах. Защита информации в архивных файлах. Программы «взлома» паролей в офисных документах, архивах. Программы «взлома» паролей в офисных документах, архивах.	Освоить программы паролей файлов офисных приложений и архив.
Лабораторная работа 3. Основы криптографической защиты информации. Симметричные алгоритмы.	Криптография. Ключ. Криптоанализ. Кодирование. Симметричные криптосистемы Шифры перестановки. Шифры простой замены. Шифры сложной замены	Процесс шифрования.
Лабораторная работа 4. Основы криптографической защиты информации. Асимметричные алгоритмы.	Асимметричные криптосистемы. Схема шифрования Эль Гамаля. Алгоритм Диффи-Хелмана. Криптосистема шифрования данных RSA.	Процесс шифрования.
Лабораторная работа 5. Программное обеспечение защиты информации.	Основные функции ПО. Генерировать ключи шифрования и сохранить их дискете (диске). Зашифровать информацию, используя полученные ключи. Передать информацию (скопировать на другой носитель) защищенную ключом.	Процесс шифрования.
Лабораторная работа 6. Хранение сведений о пользователе на сервере.	Создайте уникальный ключ, идентифицирующий пользователя. Сохраните созданный ключ на клиентском компьютере в виде файла cookie. Создайте на сервере файл для хранения сведений о пользователе. Сохраните сведения о пользователе на сервере, используя созданный уникальный ключ в качестве индекса.	Создание уникальных ключей для идентификации пользователей.
Модуль 2		
Лабораторная работа 7. Создания файлов для хранения	В Visual Studio создайте XML-файл, содержащий примерные значения в полях данных, которые предназначены для хранения сведений о пользователе. Сгенерируйте на основе XML-файла	Сохранение сведений пользователе на сервере.

сведений о пользователе	схему XML. Схема XML позволяет в наборе данных ссылаться по имени на данные, хранящиеся в XML-файле. Задайте поле ключа в схеме XML, чтобы использовать его с методом Find для поиска записей в наборе данных. Прочитайте содержимое схемы XML и XML-файла в набор данных.	Извлечение сведений о пользователе из набора данных.
Лабораторная работа 8. Проверка наличия поддержки дополнительных возможностей.	Добавьте к приложению Web-форму с именем Default.aspx и сделайте ее начальной страницей приложения. Добавьте к созданной Web-форме следующий обработчик события Page_Load.	Создание приложения Advanced Features. Готовая Web-форма.
Лабораторная работа 9. Аутентификация и авторизация пользователей	Войдите на сервер как администратор. Выберите из меню Start (Пуск) пункт Administrative Tools\Computer Management (Администрирование\Управление компьютером), чтобы запустить консоль Computer Management. Выберите в списке слева элемент Local Users And Groups (Локальные пользователи и группы), затем папку Users, чтобы открыть список авторизованных пользователей для этого компьютера. В списке справа дважды щелкните левой кнопкой анонимную учетную запись с именем в форме IUSER_имя_компътера - оснастка Computer Management откроет окно свойств учетной записи.	Web-форма.
Лабораторная работа 10. Включение аутентификации Windows	Создайте новый проект Web-приложения. Если проект использует Visual Basic-NET, измените элемент, определяющий авторизацию следующим образом (см, строку, выделенную полужирным шрифтом в HTML-коде), а если Visual C# , то следующий элемент необходимо добавить целиком. Добавьте к коду начальной Web-формы проекта следующее HTML-определение таблицы Переключите окно формы в режим Design и добавьте к объекту кода начальной Web-формы следующие строки.	Web-форма.
Модуль 3		
Лабораторная работа 11. Аутентификация Forms.	В файле Web.config установите режим аутентификации в «Forms». Создайте Web-форму для сбора учетных данных. Создайте файл или БД для хранения имен и паролей пользователей. Напишите код, добавляющий сведения о новых пользователях в файл или БД. Напишите код, выполняющий аутентификацию пользователей с применением файла или БД со сведениями о пользователях.	Web-форма.
Лабораторная работа 12. Сохранение сведений о пользователе.	Создайте новую Web-форму и назовите ее Background.aspx. Поместите на Web-форму серверный элемент управления DropDownList, элементы списка которого задают различные цвета фона. Проще всего для этого использовать режим HTML (а не Design), поскольку в нем удается	Создание Web-формы.

	быстро создавать элементы списка путем копирования-вставки соответствующего HTML-кода. Вот HTML-код, определяющий DropDownList и элементы его списка.	
Лабораторная работа 13. Сохранение сведений о пользователе.	Измените элемент <body> Web-формы так, чтобы он задавал цвет фона с помощью значений элементов списка DropDownList, используя привязку данных. Вот HTML- код модифицированного элемента <body>: <body bgColor="<%# drpBackground.SelectedItem.Value %>"> . Добавьте к обработчику события Page Load код, проверяющий наличие файла cookie и создающий его, если он не существует. Если cookie существует, этот код задаст цвет фона на основе хранящихся в нем данных. Обработчик события Page Load также использует привязку данных, чтобы обновить цвета фона.	Создание Web-формы.
Лабораторная работа 14. Создание Web-формы Mail.	Создайте новую Web-форму и назовите ее Mail.aspx. Добавьте к Web-форме текст и серверные элементы управления, показанные в следующем HTML-коде.	Создание Web-формы.
Лабораторная работа 15. Создание Web-формы Mail.	Чтобы применять сокращенные имена в ссылках на члены пространства имен System. Web. Mail, поместите в начало модуля Web-формы следующие операторы: Visual Basic .NET Imports System.Web.Mail Visual C# using System. Web.Mail. Добавьте к обработчику события butSend_Click для создания объекта MailMessage и отправки сообщения с сервера.	Создание Web-формы.
Лабораторная работа 16. Создание пользовательского интерфейса на основе фреймов.	Создайте новую HTML-страницу и назовите ее Contents.htm. Добавьте к странице Contents следующие гиперссылки. Добавьте к странице Contents следующий сценарий. Создайте набор фреймов для отображения страниц проекта. Для этого из меню Project выберите команду Add New Item, затем из списка Templates выберите Frameset и при- свойте новому файлу имя Frameset.htm, Щелкните Open - Visual Studio откроет диалоговое окно Select A Frameset Template. Выберите для набора фреймов шаблон Banner And Content и шелкните OK. Visual Studio откроет пустой набор фреймов в окне Design.Щелкните правой кнопкой крайний слева фрейм и выберите из контекстного меню команду Set Page For Frame — Visual Studio откроет диалоговое окно Select Page.В диалоговом окне Select Page укажите файл Contents.htm и щелкните ОК, чтобы назначить страницу Contents для отображения в этом фрейме. Назначьте страницу с набором фреймов начальной страницей приложения. Для этого в окне Solution Explorer шелкните правой кнопкой файл Frameset.htm и выберите из контекстного меню команду Set As Start Page.	Создание Web-формы.

5. **Образовательные технологии**

Сочетание традиционных образовательных технологий в форме лекции с интерактивными семинарскими занятиями и компьютерными автоматизированными информационными технологиями при выполнении лабораторных работ и проведении контрольных мероприятий (экзаменов, зачетов, промежуточного тестирования). Оценка качества освоения материала дисциплины складывается из оценки ответа на экзамене, оценки выполнения практической работы, представляемой на экзамен, оценки полноты и качества конспекта, оценки полноты и качества выполнения заданий на самостоятельную работу.

6. Учебно-методическое обеспечение самостоятельной работы студентов

Учебно-методические пособия для самостоятельной работы

1. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. 6-е издание. – М.: Издательский центр "Академия". 2012.
2. Microsoft Corporation M59 Разработка Web-приложений на Microsoft Visual Basic NET и Microsoft Visual C#. NET. Учебный курс MCAD/MCSD/Пер. с англ. – М.: Русская Редакция, 2003. 704 с.
3. Кузнецов И.Н. Информация: сбор, защита, анализ. Учебник по информационно-аналитической работе". – М.: Наука, 2012. 150 с.

Задания для самостоятельной работы

Разделы и темы для самостоятельного изучения	**Виды и содержание самостоятельной работы**
Тема 1. Криптографические протоколы.	Элементы протоколов. Введение в протоколы. Передача информации с использованием симметричной криптографии. Однонаправленные функции. Однонаправленные хэш-функции Передача информации с использованием криптографии с открытыми ключами. Цифровые подписи и шифрование. Генерация случайных и псевдослучайных последовательностей.
Тема 2. Основные протоколы	Обмен ключами. Удостоверение подлинности. Формальный анализ протоколов проверки подлинности и обмена ключами. Разделение секрета. Совместное использование секрета. Криптографическая защита баз данных.
Тема 3. Промежуточные протоколы.	Служба меток времени. Подсознательный канал. Неотрицаемые цифровые подписи. Подписи уполномоченного свидетеля. Подписи по доверенности. Групповые подписи. Подписи с обнаружением подделки.

	Вычисления с зашифрованными данными. Вручение битов. Подбрасывание «честной» монеты. Мысленный покер. Однонаправленные сумматоры. Раскрытие секретов «все или ничего». Условие вручение ключей.
Тема 4. Развитые протоколы.	Доказательство с нулевым знанием. Использование доказательства с нулевым знанием для идентификации. Слепые подписи. Личностная криптография с открытыми ключами. Рассеянная передача. Рассеянные подписи. Одновременная подпись контракта. Электронная почта с подтверждением. Одновременный обмен с секретами.
Тема 5. Эзотерические протоколы.	Безопасные выборы. Безопасные вычисления с несколькими участниками. Анонимная широковещательная передача сообщений. Электронные наличные.
Тема 6. Длина ключа.	Длина симметричного ключа. Длина открытого ключа. Сравнение длин симметричных и открытых ключей. Какова должна быть длина ключа?
Тема 7. Управление ключами.	Генераций ключей. Нелинейные пространства ключей. Передача ключей. Проверка ключей. Использование ключей обновление ключей. Хранение ключей. Резервные ключи. Скомпрометированные ключи. Время жизни ключей. Разрушение ключей. Управление открытыми ключами.
Тема 8. Типы алгоритмов и криптографические режимы.	Режим электронной шифровальной книги. Повтор блока. Режим сцепления блоков шифра. Потоковые шифры. Самосинхронизирующиеся потоковые шифры. Режим обратной связи по шифру. Синхронные потоковые шифры. Режим выходной обратной связи. Другие режимы блочных шифров. Выбор режима шифра. Блочные шифры против потоковых шифров.
Тема 9. Математические основы	Теория информации. Теория сложности. Теория чисел. Разложение на множители. Генерации простых чисел. Дискретные логарифмы и конечное поле.
Тема 10. Стандарт шифрования данных DES.	Описание Jgbcfybt DES. Безопасность DES. Варианты DES. Насколько безопасен сегодня DES.

7. Фонд оценочных средств, для проведения текущего контроляуспеваемости, 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	Знания, умения, навыки	Процедура освоения
ОПК-2	**Знать**: детально методы и базовые алгоритмы обработки информационных структур, методов получения новой информации.	Устный опрос, письменный опрос, тестирование.
	Уметь: использовать свои знания на практике.	Письменный опрос, лабораторная работа, коллоквиум.
	Владеть: основными методами, способами и средствами получения, хранения, переработки информации, иметь навыки работы с компьютером как средством управления информацией; пониманием концепций, синтаксической и семантической организации, методов использования современных языков программирования; пониманием концепций, базовых алгоритмов, принципов разработки и функционирования современных операционных систем.	Круглый стол.
ОПК-4	**Знать**: - правовую и нормативную базу корпоративных информационных систем отраслей; - информационную структуру и информационные ресурсы сетей отраслей как объекта защиты; - основные устройства и системы защиты объектов и информации; - основные типы методов, устройств и систем технической разведки; - методы защиты автоматизированных систем обработки данных от несанкционированного доступа к информации, в том числе: специальные технические средства опознавания пользователя ПЭВМ; - специальное программное обеспечение по защите информации ПЭВМ; - основные типы методов, устройств и систем технической разведки; специальные средства защиты от несанкционированного доступа; - организацию вычислительных работ, уменьшающую риск потери информации; - сущность, цели и принципы экономической безопасности предпринимательской деятельности, направления их практической реализации; концепцию информационной безопасности, конституционные и законодательные основы ее реализации.	Устный опрос, письменный опрос, тестирование.

	Уметь: - создавать простейшие статические web-документы в графическом многооконном режиме, так и в режиме командной строки (консоли); - применять современные системные программные средства, технологии и инструментальные средства; - применять язык C# для разработки динамических страниц сети Internet; - размещать сценарии PHP на HTML-странице; - работать в среде пакета Microsoft Visual Studio; - работать в среде пакета MSSQL Server; - использовать графические программы для создания чертежей структуры web-сайта; - использовать графические редакторы для обработки изображений, размещаемых на web-сайте.	Письменный опрос, лабораторная работа, коллоквиум.
	Владеть: - навыками работы с межсетевыми экранами и пакетами антивирусных программ; - навыками самостоятельного проектирования систем защиты информации с техническими средствами разведки, защиты информации и противодействия коммерческой разведке; - навыками работы с межсетевыми экранами и пакетами антивирусных программ; - навыками самостоятельного проектирования систем защиты информации; - с техническими средствами разведки, защиты информации и противодействия коммерческой разведке.	Круглый стол.
ПК-5	**Знать**: основные принципы работы в информационно-телекомуникационной сети Internet.	Устный опрос, письменный опрос, тестирование.
	Уметь: применять полученные знания для поиска информации о новейших научных и технологических достижениях в информационно-телекомуникационной сети Internet и других источниках.	Письменный опрос, лабораторная работа, коллоквиум.
	Владеть: навыками безопасной работы в сети Internet.	Круглый стол.
ПК-7	**Знать**: методы и приемы разработки и применения алгоритмических и программных решений в области системного и прикладного программного обеспечения.	Устный опрос, письменный опрос, тестирование.

	Уметь: - применять современные системные программные средства, технологии и инструментальные средства; - работать в среде пакета Microsoft.	Письменный опрос, лабораторная работа, коллоквиум.
	Владеть: - навыками работы в системе Windows; - навыками разработки статических и динамических страниц сети Internet; - навыками программирования на языке PHP.	Круглый стол.

7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

ОПК-2 - Способностью приобретать новые научные и профессиональные знания, используя современные образовательные и информационные технологии

Компетенция	Показатели (что обучающийся должен продемонстрировать)	Оценочная шкала		
		Удовлетворительно 51-65 баллов	**Хорошо 66-85 баллов**	**Отлично 86-100 баллов**
ОПК-2	**Знать**: детально методы и базовые алгоритмы обработки информационных структур, методов получения новой информации; **Уметь**: использовать свои знания на практике; **Владеть**: основными методами, способами и средствами получения, хранения, переработки информации, иметь навыки работы с компьютером как средством управления информацией; пониманием концепций, синтаксической и семантической организации, методов использования современных языков программирования; пониманием концепций, базовых	Демонстрация частичных знаний без грубых математических ошибок.	Умение анализировать алгоритмы решения заданий и объяснять их.	Умение обоснованно анализировать ответ, приводя собственные примеры.

	алгоритмов, принципов разработки и функционирования современных операционных систем.			

ОПК-4 - Способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Компетенция	Показатели (что обучающийся должен продемонстрировать)	Оценочная шкала		
		Удовлетворительно 51-65 баллов	Хорошо 66-85 баллов	Отлично 86-100 баллов
ОПК-4	**Знать**: - правовую и нормативную базу корпоративных информационных систем отраслей; - информационную структуру и информационные ресурсы сетей отраслей как объекта защиты; - основные устройства и системы защиты объектов и информации; - основные типы методов, устройств и систем технической разведки; - методы защиты автоматизированных систем обработки данных от несанкционированного доступа к информации, в том числе: специальные технические средства опознавания пользователя ПЭВМ; - специальное программное обеспечение по защите информации ПЭВМ; - основные типы	Демонстрация частичных знаний без грубых математических ошибок.	Умение анализировать алгоритмы решения заданий и объяснять их.	Умение обоснованно анализировать ответ, приводя собственные примеры.

	методов, устройств и систем технической разведки; специальные средства защиты от несанкционированного доступа; - организацию вычислительных работ, уменьшающую риск потери информации; - сущность, цели и принципы экономической безопасности предпринимательской деятельности, направления их практической реализации; концепцию информационной безопасности, конституционные и законодательные основы ее реализации. **Уметь**: - создавать простейшие статические web-документы в графическом многооконном режиме, так и в режиме командной строки (консоли); - применять современные системные программные средства, технологии и инструментальные средства; - применять язык C# для разработки динамических страниц сети Internet; - размещать сценарии PHP на HTML-странице; - работать в среде пакета Microsoft			

	Visual Studio; - работать в среде пакета MSSQL Server; - использовать графические программы для создания чертежей структуры web-сайта; - использовать графические редакторы для обработки изображений, размещаемых на web-сайте. **Владеть**: - навыками работы с межсетевыми экранами и пакетами антивирусных программ; - навыками самостоятельного проектирования систем защиты информации с техническими средствами разведки, защиты информации и противодействия коммерческой разведке; - навыками работы с межсетевыми экранами и пакетами антивирусных программ; - навыками самостоятельного проектирования систем защиты информации; - с техническими средствами разведки, защиты информации и противодействия коммерческой разведке.			

ПК-5 - Способностью осуществлять целенаправленный поиск информации о новейших научных и технологических достижениях в информационно-телекомуникационной сети «Интернет» и других источниках

Компетенция	Показатели (что обучающийся должен продемонстрировать)	Оценочная шкала		
		Удовлетворительно 51-65 баллов	Хорошо 66-85 баллов	Отлично 86-100 баллов
ПК-5	**Знать**: основные принципы работы в информационно-телекомуникационной сети Internet. **Уметь**: применять полученные знания для поиска информации о новейших научных и технологических достижениях в информационно-телекомуникационной сети Internet и других источниках. **Владеть**: навыками безопасной работы в сети Internet.	Демонстрация частичных знаний без грубых математических ошибок.	Умение анализировать алгоритмы решения заданий и объяснять их.	Умение обоснованно анализировать ответ, приводя собственные примеры.

ПК-7 - Способностью к разработке и применению алгоритмических и программных решений в области системного и прикладного программного обеспечения

Компетенция	Показатели (что обучающийся должен продемонстрировать)	Оценочная шкала		
		Удовлетворительно 51-65 баллов	Хорошо 66-85 баллов	Отлично 86-100 баллов
ПК-7	**Знать**: методы и приемы разработки и применения алгоритмических и программных решений в области системного и прикладного программного обеспечения. **Уметь**: - применять современные системные программные средства, технологии	Демонстрация частичных знаний без грубых математических ошибок.	Умение анализировать алгоритмы решения заданий и объяснять их.	Умение обоснованно анализировать ответ, приводя собственные примеры.

	и инструментальные средства; - работать в среде пакета Microsoft. **Владеть**: - навыками работы в системе Windows; - навыками разработки статических и динамических страниц сети Internet; - навыками программирования на языке PHP.			

Если хотя бы одна из компетенций не сформирована, то положительная оценки по дисциплине быть не может.

7.3. Типовые контрольные задания
Примерный перечень контрольных вопросов и заданий

Контрольная работа 1

1. Дать определение информационной безопасности и охарактеризовать ее цели, задачи и структуру.

2. Определить место информационной безопасности в структуре информационного права.

3. Проанализировать современные проблемы информационной безопасности предпринимательской деятельности.

4. Описать порядок охраны информационных ресурсов открытого доступа.

5. Охарактеризовать порядок защиты информационных ресурсов ограниченного доступа.

6. Определить критерии ценности информационных ресурсов и длительности сохранения ими этой характеристики.

Контрольная работа 2

1. Проанализировать содержание понятия разрешительной системы доступа персонала к конфиденциальным сведениям фирмы.

2. Проанализировать состав показателей (граф и зон) перечня конфиденциальных сведений фирмы, обосновать целевое назначение показателей и их взаимосвязь.

3. Регламентировать в виде фрагмента инструкции порядок доступа персонала к электронным конфиденциальным документам фирмы.

4. Обосновать критерии выделения конфиденциальных документов из общего потока поступающих документов.

5. Обосновать целесообразность состава процедур, сопровождающих автоматизированный учет конфиденциальных документов.

6. Составить графическую схему перемещения электронной и традиционной учетной карточки конфиденциального документа.

7. Обосновать состав показателей учетной карточки (по выбору преподавателя) и правила их заполнения

8. Сравнить способы учета конфиденциальных документов, изготовленных на дискете, выявить критерии определения эффективности каждого из способов.

Контрольная работа 3

1. Сравнить способы учета электронных конфиденциальных документов, передаваемых по линии защищенной компьютерной связи, выявить критерии определения эффективности каждого из способов.

2. Проанализировать особенности контроля за исполнением конфиденциальных документов, его организационное и технологическое отличие от контроля открытых документов.

3. Классифицировать состав бумажных и технических носителей информации, применяемых для составления деловой (управленческой) и технической конфиденциальной документации.

4. Проанализировать особенности текста конфиденциального документа.

5. Дать графическую схему расположения специфических реквизитов формуляра конфиденциального документа, описать порядок оформления реквизитов.

6. Регламентировать в виде фрагмента инструкции порядок работы исполнителей с конфиденциальными документами.

7. Проанализировать пути использования существующих средств копирования и тиражирования документов для изготовления экземпляров и копий конфиденциальных документов.

8. Обосновать необходимость реквизитов, указываемых на лицевой и оборотной стороне пакета (конверта) с конфиденциальным документом.

9. Сформулировать возможности, трудности и направления использования электронной почты для передачи конфиденциальных документов.

10. Составить фрагмент номенклатуры дел, содержащих конфиденциальные документы.

Контрольная работа 4

1. Регламентировать в виде фрагмента инструкции порядок формировании вдела электронных конфиденциальных документов.

2. Проанализировать задачи защиты информации, которые должны быть решены при формировании и оформлении дел с конфиденциальными документами.

3. Проанализировать целесообразность, назначение и порядок оформления реквизитов акта об уничтожении документов и дел.

4. Классифицировать способы и средства физического уничтожения документов, изготовленных на носителях различных типов.

5. Проанализировать пути поиска документов и дел, не обнаруженных при проверке их наличия, дать рекомендации, повышающие эффективность поиска и предотвращающие утрату документов и дел.

6. Составить план эвакуации и охраны конфиденциальных документов и дел при возникновении угрозы экстремальной ситуации, регламентировав способы обеспечения их сохранности при упаковке и транспортировке документов и дел, не обнаруженных при проверке их наличия, дать рекомендации, повышающие эффективность поиска и предотвращающие утрату документов и дел.

7. Составить план эвакуации и охраны конфиденциальных документов и дел при возникновении угрозы экстремальной ситуации, регламентировав способы обеспечения их сохранности при упаковке и транспортировке.

Вопросы к зачету

1. Предмет, цели и задачи дисциплины.

2. Основные определения и понятия.

3. Законодательство в области информационной безопасности и защиты данных.

4. Структуры и нормативные акты, их направления».

5. Классификация нормативных актов в области ИБ и ЗД.

6. Государственные органы, регулирующие вопросы информационной безопасности.

7. Классификация информации по степени ее защиты.

8. Доктрина информационной безопасности РФ.

9. Законодательство и нормативные акты Российской Федерации.

10. Классификация информационных ресурсов, характеристика и основные свойства.

11. Информационные ресурсы в современных условиях, требования к ним, надежность (достоверность) информации и защиты от несанкционированного доступа.

12. Классификация и анализ угроз информационной безопасности корпоративным системам.

13. Уровни защиты информации: правовой; организационный; аппаратно-программный; криптографический

14. Классификация криптографических методов.

15. Традиционные (симметричные) криптосистемы.

16. Блоковые и поточные шифры.

17. Стойкость криптосистем.
18. Американский стандарт шифрования данных DES.
19. Отечественный стандарт криптографической защиты ГОСТ 28147-89.
20. Асимметричные криптосистемы.
21. Математические основы криптографии с открытым ключом.
22. Криптосистема RSA.
23. Криптосистема Эль Гамаля.
24. Криптосистемы без передачи ключей.
25. Управление ключами.
26. Методы генерации, хранения и распределения ключей.
27. Протоколы управления ключами
28. Аппаратно-программные решения защиты информации в информационных системах.
29. Аппаратно-программные средства контроля доступа.
30. iButton.
31. Смарт-карты.
32. Устройства ввода на базе USB-ключей.
33. Proximity.
34. Биометрические УВИП
35. Комбинированные устройства ввода.
36. Электронные замки.
37. Инфраструктура открытых ключей.
38. Цифровые сертификаты.
39. Электронная цифровая подпись (ЭЦП).
40. Однонаправленная хэш-функция.
41. Идентификация и аутентификация объектов сети.
42. Идентификация и подтверждение подлинности пользователей сети.
43. Математические методы обеспечения защиты от несанкционированного доступа и конфиденциальности».
44. Исторический очерк развития криптографии.
45. Криптография древнего периода.
46. Криптография арабского мира.
47. Криптография в эпоху Возрождения (XIV--XVI вв.).
48. Криптография в XVII--XVIII веках.
49. Криптография в XIX веке.
50. Криптография в XX веке.
51. О криптографии нового времени.
52. Криптография: понятия, подходы, направления исследований.
53. Базовая терминология.

54. Основные алгоритмы шифрования.

55. Цифровые подписи.

56. Криптографические хэш-функции.

57. Криптографические генераторы случайных чисел.

58. Обеспечиваемая шифром степень защиты.

59. Криптоанализ и атаки на криптосистемы.

60. Межсетевое экранирование.

61. Принципы построения и функционирования межсетевых экранов (МЭ). Классификация МЭ.

62. Особенности межсетевого экранирования на различных уровнях модели Криптография и криптоанализ в авторизации, аутентификации и в обмене информации.

63. Основные понятия и принципы криптографии.

64. Симметричные криптосистемы.

65. Асимметричные криптосистемы.

66. Электронная цифровая подпись.

67. Управление ключами в криптографических системах защиты информации.

68. Особенности реализация криптографических методов.

69. Федеральная инфраструктура открытых ключей.

70. Направления исследований в области криптосистем.

71. Средства антивирусной защиты.

72. Классификация вирусов и средств защиты.

73. Виды антивирусных программных продуктов.

74. Характеристика наиболее популярных антивирусных пакетов.

75. Архитектура системы защиты информации (СЗИ).

76. Этапы создания СЗИ. Виды обеспечения СЗИ.

77. Принципы разработки СЗИ.

78. Информационная безопасность в глобальном информационном пространстве Интернет.

79. Безопасная интеграция в Интернет.

80. Программные и технологические решения».

81. Угрозы и риски интернет-технологий.

82. Стандартизация информационной безопасности в Интернет.

83. Программно-аппартные технологии Интернет.

84. Брандмауэры.

85. Программное обеспечение защиты информации в Интернет.

86. Основные понятия и принципы криптографии.

87. Симметричные криптосистемы.

88. Асимметричные криптосистемы.

89. Электронная цифровая подпись.

90. Управление ключами в криптографических системах защиты информации.
91. Особенности реализация криптографических методов.
92. Серверы доступа (брандмауэры) Cisco ASA5500.
93. Средства обнаружения вторжений IDS 4200.

7.4. 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 - 30 баллов,
- участие на практических занятиях - 40 баллов,
- выполнение домашних работ–30 баллов.

Промежуточный контроль по дисциплине включает:
- устный опрос - 40 баллов,
- письменная контрольная работа - 30 баллов.

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

а) основная литература:

4. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. 6-е издание. – М.: Издательский центр "Академия". 2012.
5. Microsoft Corporation M59 Разработка Web-приложений на Microsoft Visual Basic NET и Microsoft Visual C# .NET. Учебный курс MCAD/MCSD/Пер. с англ. – М.: Русская Редакция, 2003. – 704 с.
6. Кузнецов И.Н. Информация: сбор, защита, анализ. Учебник по информационно-аналитической работе". – М.: Наука, 2012. 150 с.
7. Савченко Е. Кто, как и зачем следит за вами через интернет. – М.: Мир, 2012. 100с.
8. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности. 2-е изд. М. 2014-130 с.
9. Бауэр Ф. Расшифрованные секреты. Методы и принципы криптологии. – М.: Мир, 2007. 550 с.
10. Мазаник С. Безопасность компьютера: защита от сбоев, вирусов и неисправностей. – М.: Мир. 2007. 256 с.
11. Мельников В. П., Информационная безопасность и зашита информации: учебное пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков. – М.: Академия, 2011.
12. Тарасов М. А., Электронное правительство и информационная безопасность: учебное пособие – М.: ГАЛАРТ. 2011.

13. Бачило И. Л., Информационное право: учебник – М.: Юрайт// ЭБС ЛАНЬ, 2011.
14. Шаньгин В. Ф., Защита информации в компьютерных системах и сетях. – М.: "ДМК Пресс", 2012.
15. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации. – М.: ИНФРА. 2001.
16. Закон Российской Федерации от 11.03.1992 № 2487-1 «О частной детективной и охранной деятельности» // Российская газета. – 1992. – № 100.
17. Ковалева Н. Н., Информационное право России: учеб. пособие – М.: Дашков и К, 2007.
18. Ищейнов В. Я., Мецатунян М. В., Защита конфиденциальной информации: учеб. пособие для вузов/ В. Я. Ищейнов В. Я., М. В. Мецатунян. – М.: ФОРУМ, 2009
19. Некраха А. В., Шевцова Г. А., Организация конфиденциального делопроизводства и защита информации: учеб. пособие для вузов/ А. В. Некраха, Г. А. Шевцова. – М.: Академ. Проект, 2007
20. Шаньгин В. Ф Защита компьютерной информации. Эффективные методы и средства. Учебное пособие. ДМК Пресс, 2010.
21. Компьютерные сети. 4-е изд. Э.Таненбаум. – СПб.: Питер, 2003. 992 с.
22. Кучерявский С.В., Суранов А.Я. Основы сетевых технологий. – Барнаул: Изд-во Алтайского университета, 2004.
23. Блэк У. Интернет: протоколы безопасности. Учебный курс. – СПб.: Питер, 2001.

б) дополнительная литература:

1. В.Олифер, Н.Олифер. Компьютерные сети. Принципы, технологии, протоколы – СПб: "Питер", 2003.
2. Вычислительные системы, сети и телекоммуникации: Учеб. для вузов/ А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко; Под ред. А. П. Пятибратова. 2-е изд., перераб. и доп. – М.: Финансы и статистика, 2003.
3. М.А.Мамаев. Телекоммуникационные технологии: Сети TCP/IP. Учебное пособие – Владивосток: Изд-во ВГУЭиС, 1999.
4. Компьютерные системы и сети: Учеб. пособие для вузов / Под ред. В. П. Косарева, Л. В. Еремина. – М.: Финансы и статистика, 1999.
5. Голдовский И. Безопасность платежей в Интернете. – СПб.: Питер, 2001.
6. Крейн Д. и др. Ajax в действии. – М.: Вильямс, 2006.
7. Мельников Д.А. Информационные процессы в компьютерных сетях. Протоколы, стандарты, интерфейсы, модели: – М.: КУДИЦ-ОБРАЗ, 2001, 256 с.
8. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. Изд. 2-е, перераб., – М.: Радио и связь, 2001, 376 с.

9. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия-Телеком, 2000, 452 с.

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

http://eqworld.ipmnet.ru/ru/solutions/ode.htm Мир математических уравнений библиотека;
http://www.poiskknig.ru/ поиск электронных книг;
http://discopal.ispras.ru/ru.book-advanced-algorithms.htm;
www.mathnet.ru - общероссийский математический портал;
www.library.kemsu.ru - электронный каталог НБ КемГУ;
www.elibrary.ru - научная электронная библиотека;
www.lib.mexmat.ru - электронная библиотека механико-математического факультета МГУ;
www.newlibrary.ru - новая электронная библиотека;
www.edu.ru - федеральный портал российского образования.

10. Методические указания для обучающихся по освоению дисциплины

Для понимания материала и качественного его усвоения рекомендуется следующая последовательность действий:

1. После прослушивания лекции и окончания учебных занятий, при подготовке к занятиям следующего дня, нужно сначала просмотреть и обдумать текст предыдущей лекции – 10-15 минут.

2. В течение недели выбрать время – 1 час для работы с литературой по программированию и анализу алгоритмов.

3. При подготовке к лабораторным занятиям, необходимо сначала прочитать основные понятия, изучить алгоритмы по теме домашнего задания. При написании программы нужно сначала понять, что требуется, какой теоретический материал нужно использовать, наметить план решения задачи. Алгоритм решения задачи – это не программа ее решения, а способ дать человеку (а не машине) представление о структуре алгоритма, о смысле его шагов и их логической взаимосвязи. Поэтому шаги алгоритма должны описываться в терминах тех объектов и отношений между ними, о которых идет речь в условии задачи (это, конечно, не исключает использования математической и другой условной символики). Структура алгоритма станет более ясной, если ее описывать в наглядной и достаточно формализованной (напоминающей конструкции языка программирования) форме. Поэтому требуемой формой описания алгоритма в данном лабораторном практикуме является либо графическое представление алгоритма на языке блок-схем, либо на специальном языке описания алгоритмов, например школьном алгоритмическом языке.

4. Основная часть теоретического материала курса дается в ходе лекционных занятий, хотя часть материала может изучаться на лабораторных занятиях, либо самостоятельно по учебной литературе.

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

При осуществлении образовательного процесса по дисциплине «Алгоритмы и анализ сложности» рекомендуется использовать следующие информационные технологии.

Во-первых, должны проводиться занятия с компьютерным тестированием, что приучит студентов хорошо ориентироваться с работой на компьютере для выполнения заданий.

Во-вторых, демонстрационный материал также будет показан с помощью мультимедийных устройств и интерактивной доски.

В-третьих, компьютерные классы с набором лицензионного базового программного обеспечения для проведения занятий.

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

При освоении дисциплины для выполнения лабораторных работ необходимы классы персональных компьютеров с приложениями программирования на языках C/C++, а также учебные аудитории для проведения лекционных занятий.