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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Информационная безопасность и защита информации

Кафедра дискретной математики и информатики **факультета математики и компьютерных наук**

Образовательная программа
02.03.02 - Фундаментальная информатика и информационные технологии

Профиль подготовки
Информатика и компьютерные науки

Уровень высшего образования
бакалавират

Форма обучения
очная

Статус дисциплины: вариативная

Махачкала, 2017

Рабочая программа дисциплины «Информационная безопасность и защита информации» составлена в 2017 году в соответствии с требованиями ФГОС ВО по направлению подготовки 02.03.02 - Фундаментальная информатика и информационные технологии (уровень бакалавриат)
от 12 марта 2015г. № 224.

Разработчик: кафедра дискретной математики и информатики,
док. т. н., проф. Алибеков Б.И.

Рабочая программа дисциплины одобрена:
на заседании кафедры от 5 мая 2017 г., протокол № 9
Зав. кафедрой _____ Магомедов А.М.
(подпись)

на заседании Методического совета факультета математики и компьютерных наук от 19 мая 2017 г., протокол № 9.
Председатель _____ Меджидов З.Г.
(подпись)

Рабочая программа дисциплины согласована с учебно-методическим управлением «22» мая 2017г. _____
(подпись)

Аннотация рабочей программы дисциплины

Дисциплина «**Информационная безопасность и защита информации»** входит в вариативную часть образовательной программы бакалавриата по направлению **02.03.02 - Фундаментальная информатика и информационные технологии.**

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

Рабочая программа дисциплины «**Информационная безопасность и защита информации»** составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего профессионального образования бакалавриата по направлению **02.03.02 - Фундаментальная информатика и информационные технологии.**

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: **общепрофессиональными компетенциями - (ОПК-4)**, профессиональных **(ПК-7), (ПК-8).**

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: дисциплина изучается один семестра - 8 семестр – 32 ч. лекций, 32 ч. лаб. - экзамен.

Объем дисциплины -144 ч. (аудиторная -64 ч., самостоятельная -44 ч., экз 36 ч. 4 зачетных единиц (3 модуля и экзамен) 8 семестр)

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	32	32	0			44	экзамен

1. Цели и задачи дисциплины, и ее место в учебном процессе

Основные цели преподавания 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 з ащиты информации. Это достигается с помощью лекций и выполнения лабораторных работ, а также самоподготовки студентов.

Рабочая программа по дисциплине «Информационная безопасность и защита информации» составлен в соответствии с требованиями Государственного образовательного стандарта высшего профессионального образования по направлению бакалавриата . **02.03.02 - Фундаментальная информатика и информационные.**

Ожидаемые результаты:

В результате освоения дисциплины обучающиеся должен:

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, минимизирующую риск потери информации;

-сущность, цели и принципы экономической безопасности предпринима тельской деятельности, направления их практической реализации;

-концепцию информационной безопасности, конституционные и зако нодательные основы ее реализации;

Уметь:

- создавать простейшие статические web-докуграфическом многооконном режиме, так и в режиме командной строки (консоли);
- применять современные системные программные средства, технологии и инструментальные средства;
- применять язык PHP для разработки динамических страниц сети Internet;
- размещать сценарии PHP на HTML-странице; - работать в среде пакета Microsoft Visual Studio;
- работать в среде пакета MS SQL 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;**

-DataGridView; навыками работы с межсетевыми экранами и пакетами антивирусных программ;

2. Место дисциплины в структуре ООП бакалавриата (специалиста, магистратуры)

Дисциплина «Информационная безопасность и защита информации» входит в вариативная часть образовательной программы бакалавриата по направлению 02.03.02 - Фундаментальная информатика и информационные технологии.

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) .

Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы 02.03.02 - Фундаментальная информатика и информационные Целью освоения дисциплины " **Информационная безопасность и защита информации** " является: изучение основных приемов и методов разработки Web-страниц с интерактивными элементами. В результате освоения ООП бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине:

Компетенции	Формулировка компетенции из ФГОС ВО	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)
(ОПК-4);	способностью решить стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологии 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, минимизирующую риск потери информации;** сущность, цели и принципы

		экономической безопасности предпринима тельской деятельности, направления их практической реализации; концепцию информационной безопасности, конституционные и зако нодательные основы ее реализации; Уметь: - создавать простейшие статические web-докуграфическом 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 MS SQL 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;** DataGridView; 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 в системе Windows; - навыками разработки статических и динамических страниц сети Internet - навыками программирования на языке PHP
(ПК-7)	способностью разработать и реализовать процессы жизненного цикла информационных схем, программного обеспечения, сервисов систем информационных технологии , а так же методы и механизмы оценки и анализа функционирования средств и и систем информационных технологии	Знать: методы охраны зданий, помещений, оборудования, документации и персонала в обычных и экстремальных ситуациях, проведения охранных мероприятий в том числе с использованием соответствующих технических средств; методику защиты информации при проведении основных деловых мероприятий (переговоры, прием посетителей), в рекламной и выставочной деятельности, работе кадровой службы и др.; - протоколы обмена информацией web-серверов и клиентских браузеров; - основы сетевых технологий, TCP/IP и принципы функционирования сети Интернет Уметь: **использовать программное обеспечение для надежного уничтожения информации;** **создавать архивы;** **применять программное обеспечение для защиты от "вирусов";** **организовать вычислительную работу с минимумом риска потери информации.** Владеть: **законодательными мерами по защите информации;** методами охраны зданий, помещений, оборудования, документации и персонала в обычных и экстремальных ситуациях, проведения охранных мероприятий в том числе с использованием соответствующих технических средств;

		- приемами разработки web-приложений с использованием баз данных
(ПК-8)	-способностью применять на практике международные и профессиональные стандарты информационных технологий, современные парадигмы и методологии, инструментальные и вычислительные средства.	Знать: - этапы производства программного продукта; - методы и средства тестирования программ; - способы обеспечения информационной безопасности контента сетевых ресурсов жизненного цикла программного обеспечения; Качество программного обеспечения; Технология вычислительных систем; Системное администрирование; Системная интеграция; Основы программной инженерии; Верификация и испытания программного обеспечения; Встроенные системы; Распределенные системы; Управление безопасностью ИТ; Управление инфокоммуникациями; Уметь использовать : криптографические методы защиты информации; протоколы взаимной аутентификации объектов сетей; методы организации систем защиты информации. методы организации систем защиты информации. Владеть: **с техническими средствами разведки, защиты информации и противодействия коммерческой разведке;** **законодательными мерами по защите информации;** методами охраны зданий, помещений, оборудования, документации и персонала

		в обычных и экстремальных ситуациях, проведения охранных мероприятий, в том числе с использованием соответствующих технических

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет Общая учебная нагрузка -144 ч. (аудиторная -64 ч., самостоятельная -44 ч., экз 36 ч. 4 зачетных единиц.

4.2. Структура дисциплины.

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*
			лек.	Лаб.	Сам. р.	Конт р.	
Модуль 1							
Тема 1. Предмет, цели и задачи дисциплины . Основные определения и понятия. [1-5]	8	1	2	2	2		
Тема 2 Общая проблема информационной безопасности информационных систем. [1-5]	8	2	2	2	2		
Тема 3. Классификация информационных ресурсов, характеристика и основные свойства[1-5]	8	3	2	2	2		Прием лабораторных работ
Тема 4 Классификация и анализ угроз информационной безопасности корпоративным системам. [1-5]	8	4	2	2	2		Прием лабораторных работ
Тема5. . Классификация криптографических методов [1-5]	8	5	2	2	2		Прием лабораторных работ
Тема 6. Асимметричные криптосистемы. [1-5]	8	6	2	2	2		Прием лабораторных работ
Модуль 1			12	12	12		36
Модуль 2							
Тема 7. Управление ключами. [1-5]	8	7	2	2	4		Прием лабораторных работ
Тема 8 Аппаратно-программные решения защиты информации в информационных системах»	8	8	2	2	4		Прием лабораторных работ
Тема 9 Идентификация и аутентификация объектов сети. [1-5]	8	9	2	2	2		Прием лабораторных работ

Тема 10 Математические методы обеспечения защиты от несанкционирован-ного доступа и конфиденциальности [1-5]	8	10	2	2	2		Прием лабораторных работ
Тема 11. Межсетевое экранирование. Принципы построения и функционирования межсетевых экранов [1-5]	8	11	2	2	4		Прием лабораторных работ
			10	10	16		36
Модуль 3							
Тема 12. Криптография и криптоанализ в авторизации, аутентификации и в обмене информации[1-5]	8	12	2	2	2		
Тема 13. Средства антивирусной защиты	8	13	2	2	4		Прием лабораторных работ
Тема 14. Архитектура системы защиты информации). [1-5]	8	14	2	2	4		Прием лабораторных работ
Тема 15. . Информационная безопасность в глобальном информационном простран-стве Интернет. Безопасная интеграция в Интернет. Программные и технологические решения[1-5]	8	15	2	2	2		Прием лабораторных работ
Тема 16 . Серверы доступа (брандмауэры) [1-5]	5	16	2	2	4		Прием лабораторных работ
Модуль 3			10	10	16		36
Подготовка к экзамену						36	
			32	32	44	36	Экзамен

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

Модуль1.

Лекция 1. Предмет, цели и задачи дисциплины “Информационная безопасность и защита информации”. Основные определения и понятия. [1-5]

Лекция 2 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. [1-5]

Лекция 3. Классификация информационных ресурсов, характеристика и основные свойства. Информационные ресурсы в современных условиях, требования к ним, надежность (достоверность) информации и защиты от несанкционированного доступа. [1-5]

Лекция 4. . Классификация и анализ угроз информационной безопасности корпоративным системам. Уровни защиты информации: правовой; организационный; аппаратно-программный; криптографический[1-5]
Лекция 5. Классификация криптографических методов. Традиционные (симметричные) криптосистемы. Блоковые и поточные шифры. Стойкость криптосистем. Американский стандарт шифрования данных DES. Отечественный стандарт криптографической защиты ГОСТ 28147-89. [1-5]
Лекция 6. 6 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 [1-5]
Модуль 2
Лекция 7. «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 [1-5]
Лекция 8. Инфраструктура открытых ключей. Цифровые сертификаты. Электронная цифровая подпись (ЭЦП). Однонаправленная хэш-функция. [1-5]
Лекция 9. Идентификация и аутентификация объектов сети. Идентификация и подтверждение подлинности пользователей сети. [1-5]
Лекция 10. «Математические методы обеспечения защиты от несанкционирован-ного 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[1-5]
Лекция 11. Межсетевое экранирование. Принципы построения и функционирования межсетевых экранов (МЭ). Классификация МЭ. Особенности межсетевого экранирования на различных уровнях модели OSI [1-5]
Модуль 3
Лекция 12. «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. [1-5]
Лекция 13. Средства антивирусной защиты. Классификация вирусов и средств защиты. Виды антивирусных программных продуктов. Характеристика наиболее популярных антивирусных пакетов. [1-5]
Лекция 14. Архитектура системы защиты информации (СЗИ). Этапы создания СЗИ. Виды обеспечения СЗИ. Принципы разработки СЗИ. [1-5]
Лекция 15. «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[1-5]
Лекция 16. Серверы доступа (брандмауэры) Cisco ASA5500. Средства обнаружения вторжений IDS 4200. [1-5]

Лабораторные работы (лабораторный практикум)

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

№№ и названия разделов и тем	Цель и содержание лабораторной работы	Результаты лабраторной работы
Модуль1.		
Лабораторная работа 1 Защита баз данных на примере MS ACCESS[1-5]	Алгоритм защиты БД MS Access. Порядок выполнения и результаты работы.	Защита на уровне пароля Защита на уровне пользователя. Создать и изменеть пароль.
Лабораторная работа 2 Стандартные способы зашиты информации. [1-5]	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» [1-5]	Криптография. Ключ. Криптоанализ. Кодирование. Симметричные криптосистемы Шифры перестановки. Шифры простой замены. Шифры сложной замены	Процесс шифрование
Лабораторная работа 4.. «Основы криптографической защиты информации. Асимметричные алгоритмы». [1-5]	Асимметричные криптосистемы Схема шифрования Эль Гамаля. Алгоритм Диффи-Хелмана. Криптосистема шифрования данных RSA	Процесс шифрование
Лабораторная работа 5. Программное обеспечение защиты информации[1-5]	Основные функции ПО. Генерировать ключи шифрования и сохранить их дискете (диске)... Зашифровать информацию, используя полученные ключи.. Передать информацию (скопировать на другой носитель) защищенную ключем.	Процесс шифрование
Лабораторная работа 6. Хранение сведений о пользователе на сервере. [1-5]	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.
Модуль2		
Лабораторная работа 7. Создания файлов	В Visual Studio создайте XML-файл, содержащий примерные значения в полях данных,	Сохранение сведений о

для хранения сведений о пользователе[1-5]	которые предназначены для хранения сведений о пользователе. . Сгенерируйте на основе XML-файла 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.	пользователе на сервере Извлечение сведений о пользователе из набора данных
Лабораторная работа 8. Проверка наличия поддержки дополнительныхвозможностей[1-5]	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[1-5]	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[1-5]	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 начальнойWeb-формы проекта следующее HTML-определение таблицы Переключите окно формы в режим Design и добавьте к объекту кода начальной Web-формы следующие строки	Web-форма
Модуль3		
Лабораторная работа 11. Аутентификация Forms[1-5]	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[1-5]	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 быстро создавать элементы спис- ка путем копирования-вставки соответствующего HTML-кода. Вот HTML-код, опре- деляющий DropDownList и элементы его списка:	СозданиеWeb-формы
Лабораторная работа 13 Сохранение сведений о пользователе. [1-5]	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 ис- пользует привязку данных, чтобы обновить цвета фона.	СозданиеWeb-формы
Лабораторная работа 14. Создание Web-формы Mail[1-5]	Создайте новую Web-форму и назовите ее Mail.aspx. . Добавьте к Web-форме текст и серверные элементы управления, показанные в следую- щем HTML-коде:	СозданиеWeb-формы
Лабораторная работа 15 Создание Web-формы Mail[1-5]	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:	СозданиеWeb-формы
Лабораторная работа 16. Создание пользовательского интерфейс на основе фреймов[1-5]	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 диа-	СозданиеWeb-формы

	логовое 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 шелкните ОК, чтобы на- значить 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	

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- методические обеспечение самостоятельной работы студентов.

Самостоятельная работа студентов по подготовке к лабораторным работам, оформлению отчетов и защите лабораторных работ включает проработку и анализ теоретического материала, описание проделанной экспериментальной работы с приложением таблиц, запросов, а и также самоконтроль знаний по теме лабораторной работы с помощью нижеприведенных контрольных вопросов и заданий.

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины. Рекомендуемая литература

Разделы и темы для самостоятельного изучения	Виды и содержание самостоятельной работы
Литература. Брюс Шнайр прикладная криптография 2-издание. Протоколы, алгоритмы и исходные тексты на языке С.(Электронном варианте).	
1.Криптографические протоколы. [1-5]	Элементы протоколов.. Введение в протоколы. Передача информации с использованием симметричной криптографии. Однонаправленые фукции
2.Криптографические протоколы. [1-5]	Однонаправленные хэш-функции Передача информации с использованием криптографии с открытыми ключами. Цифровые подписи . Цифровые подписи . и

	шифрование. Генерация случайных и псевдослучайных последовательностей
3.Основные протоколы[1-5]	Обмен ключами. Удостоверение подлинности.формальный анализ протоколов проверки подлинности иобмена ключами. Разделение секрета. Совместное использование секрета. Криптографическая защита баз данных
4.Промежуточные протоколы[1-5]	Служба меток времени. Подсознательный канал. Неотрицаемые цифровые подписи.подписи уполномоченного свидетеля. Подписи по доверенности. Групповые подписи. Подписи с обнаружением подделки
5.Промежуточные протоколы[1-5]	Вычисления с зашифрованными данными. Вручение битов. Побрасывание «честной » монеты. Мысленный покер. Однонаправленные сумматоры. Раскрытие секретов «все или ничего» Условие вручение ключей.
6.Развитые протоколы. [1-5]	Доказательство с нулевым знанием. Использование доказательства с нулевым знанием для идентифии. Слепые подписи. Личностная криптография с открытыми ключами. Рассеянная передача. Рассеянные подписи. Одновременная подпись контракта.Электроная почта с подтверждением. Одновременный обмен с секретами
7.Эзоерические протоколы[1-5]	Безопасные выборы. Безопасные вычисления с несколькими участниками. Анонимная широковещательная передача сообщений. Электронные наличные.
8.Длина ключа[1-5]	Длина симметричного клбча. Длина открытого ключа. Сравнение длин симметричных и открытых ключей. Вскрытие в день рождения против однонаправленных хэш-функции. Каков должен быть длина ключа?
9.Управление ключами[1-5]	Генераций ключей. Нелинейные пространства ключей. Передача ключей. Проверка ключей. Использование ключей обновлеие ключей. Хранение ключей. Резервные ключи. Скомпрометированные ключи.время жизни ключей. Разрущение ключей. Управление открытыми клюами.
10.Типы алгоритмов и криптографические режимы. [1-5]	Режим элекронной шифревальной 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.прослаивание. блочные шифры пртив потоковых шивров.
11.Математические основы[1-5]	Теория инормации. Теория сложности. Теория чисел.
	Разложение на множители. Генерации прстых чисел. Дискретные логорифмы и конечное поле
12.Стандарт шфрование данных DES[1-5]	Описание Jgbcfybt DES.безопасность DES. Варианты DES. Насколько безопасен сегодня DES.

6.1. Содержание самостоятельной работы студентов по дисциплине

Раздел дисциплины	**Работа над дисциплиной**		
	Содержание учебного задания	Время (час)	
		Аудиторное	СРС
Темы 1 – 6 [1-5]	Подготовка к контрольной работе №1, выполнение домашних заданий. Подготовка к защите домашних заданий.		10
Темы 7 11 [1-5]	Подготовка к контрольной работе №2, выполнение домашних заданий. Подготовка к защите домашних заданий.		10
Темы 12 –16 [1-5]	Подготовка к контрольной работе №3, выполнение домашних заданий. Подготовка к защите домашних заданий.		10
Темы 1 – 16 [1-5]	Выполнение и подготовка к защите индивидуального домашнего задания.		14
	Всего		44

Материально-техническое обеспечение дисциплины (модуля)

При освоении дисциплины для выполнения лабораторных работ необходимы персональные компьютеры с набором программного обеспечения. В учебном процессе для освоения дисциплины используются следующие технические средства: - компьютеры оборудование. У каждого студента имеются электронные книги..

Программа составлена с требованием ФГОС ВО с учетом рекоммендаций и ПрООП ВО по Направлению **02.03.02 - Фундаментальная информатика и информационные** профилю подготовки Информатика и компьютерные науки

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

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

Код компетенции	**Критерии в соответствии с уровнем освоения ОП**			**Виды занятий (лекции, семинарские, практические, лабораторные)**	**Оценочные средства (тесты, творческие работы, проекты и др.)**
	пороговый (удовл.) 51-75 баллов	**базовый (хор.) 76-90 баллов**	**повышенный (отл.) 91-100 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;** **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**	Уметь: создавать простейшие статические web-докуграфическом многооконном режиме, так и в режиме командной строки - работать в среде пакета Microsoft Visual Studio; - работать в среде пакета MS SQL Server; - использовать графические программы для создания чертежей структуры web-сайта; - использовать графические редакторы для обработки изображений, размещаемых на web-сайте криптографические методы защиты информации; протоколы взаимной аутентификации объектов сетей; методы организации систем защиты информации. методы организации систем защиты информации.	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;** DataGridView; - навыками работы в системе Windows; - навыками разработки статических и динамических страниц сети Internet навыками работы с межсетевыми экранами и пакетами антивирусных программ; навыками самостоятельного проектирования систем защиты информации. **с**	**лекции** и **лабораторные**[1-5]	Контрольные работы, тесты, домашние задания.

ПК-7	Знать: методы охраны зданий, помещений, оборудования, документации и персонала в обычных и экстремальных ситуациях, проведения охранных мероприятий в том числе с использованием соответствующих технических средств; методику защиты информации при проведении основных деловых мероприятий (переговоры, прием посетителей), в рекламной и выставочной деятельности, работе кадровой службы и др.; - протоколы обмена информацией web-серверов и клиентских браузеров; - основы сетевых технологий, TCP/IP и принципы функционирования сети Интернет - основы сетевых технологий, TCP/IP и принципы функционирован	Уметь: **использовать программное обеспечение для надежного уничтожения информации;** **создавать архивы;** **применять программное обеспечение для защиты от "вирусов";** **организовать вычислительную работу с минимумом риска потери информации.**	Владеть: **законодательными мерами по защите информации;** методами охраны зданий, помещений, оборудования, документации и персонала в обычных и экстремальных ситуациях, проведения охранных мероприятий в том числе с использованием соответствующих технических средств; - приемами разработки web-приложений с использованием баз данных	**лекции** и **лабораторные**[1-5]	Контрольные работы, тесты, домашние задания

ПК-8	Знать: - этапы производства программного продукта; - методы и средства тестирования программ; - способы обеспечения информационной безопасности контента сетевых ресурсов жизненного цикла программного обеспечения; Качество программного обеспечения; Технология вычислительных систем; Системное администрирование; Системная интеграция; Основы программной инженерии; Верификация и испытания программного обеспечения; Встроенные системы; Распределенные системы; Управление безопасностью ИТ; инфокоммуникациями	Уметь: криптографические методы защиты информации; протоколы взаимной аутентификации объектов сетей; методы организации систем защиты информации. методы организации систем защиты информации.	Владеть: **с техническими средствами разведки, защиты информации и противодействия коммерческой разведке;** **законодательными мерами по защите информации;** методами охраны зданий, помещений, оборудования, документации и персонала в обычных и экстремальных ситуациях, проведения охранных мероприятий в том числе с использованием соответствующих технических средств;	**лекции** и **лабораторные**[1-5]	Контрольные работы, тесты, домашние задания

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

ОПК-4

Схема оценки уровня формирования компетенции «способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологии и с учетом основных требований информационной безопасности».

Уровень	Показатели (что обучающийся должен продемонстрировать)	Оценочная шкала		
		Удовлетворительно	Хорошо	Отлично
Пороговый	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 з ащиты информации. Это достигается с помощью лекций и выполнения лабораторных работ, а также самоподготовки студентов.	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;** **основные типы методов, устройств и систем технической разведки;** **методы защиты автоматизирован**	Уметь: создавать простейшие статические web-докуграфическом многооконном режиме, так и в режиме командной строки - работать в среде пакета Microsoft Visual Studio; - работать в среде пакета MS SQL Server; - использовать графические программы для создания чертежей структуры web-сайта; - использовать графические редакторы для	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;** DataGridView; - навыками работы в системе Windows; - навыками

		ных систем обработки данных от несанкционированного доступа к информации, в том числе: **специальные технические средства опознавания пользователя ПЭВМ;**	обработки изображений, размещаемых на web-сайте криптографические методы защиты информации; протоколы взаимной аутентификации объектов сетей; методы организации систем защиты информации. ий, размещаемых на web-сайте: - применять	разработки статических и динамических страниц сети Internet навыками работы с межсетевыми экранами и пакетами антивирусных программ; навыками самостоятельного проектирования систем защиты информации. **с техническими средствами**

ПК-7

Схема оценки уровня формирования компетенции «способностью разработать и реализовать процессы жизненного цикла информационных схем, программного обеспечения, сервисов систем информационных технологии , а так же методы и механизмы оценки и анализа функционирования средств и и систем информационных технологии»

Уровень	Показатели (что обучающийся должен продемонстрировать)	Оценочная шкала		
		Удовлетворительно	Хорошо	Отлично
Пороговый	В процессе обучения студенты должны изучить правовую базу информационной безопасности информационных систем, угрозы информационной безопасности корпоративных систем отраслей., методы защиты информации,	Знать: методы охраны зданий, помещений, оборудования, документации и персонала в обычных и экстремальных ситуациях, проведения охранных	Уметь: **использовать программное обеспечение для надежного уничтожения информации;** **создавать архивы;** **применять программное**	Владеть: **законодательными мерами по защите информации;** методами охраны зданий, помещений, оборудования, документации и персонала в

	включая криптографически е, способы защиты информации от несанкционирован ного доступа к информации и техническим ресурсам корпоративных сетей отраслей, архитектуру и методы организации систем з ащиты информации. Это достигается с помощью лекций и выполнения лабораторных работ, а также самоподготовки студентов.	мероприятий в том числе с использование м соответствующ их технических средств; методику защиты информации при проведении основных деловых мero- приятий (переговоры, прием посетителей), в рекламной и выставочной деятельности, работе кадровой службы и др.; - протоколы обмена информацией web-серверов и клиентских браузеров; - основы сетевых технологий, TCP/IP и принципы функционирова ния сети Интернет	**обеспечение для защиты от "вирусов"; организовать вычислитель ную работу с минимумом риска потери информации.** информационных объектов современными браузерами	обычных и экстремальных ситуациях, проведения охранных мероприятий в том числе с использованием соответствующ их технических средств; - приемами разработки web-приложений с использованием баз данных

ПК-8

Схема оценки уровня формирования компетенции «способностью применять на практике международные и профессиональные стандарты информационных технологий, современные парадигмы и методологии, инструментальные и вычислительные средства».

Уровень	Показатели (что обучающийся должен	Оценочная шкала		
		Удовлетворительно	Хорошо	Отлично

	продемонстрировать)			
Пороговый	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 з ащиты информации. Это достигается с помощью лекций и выполнения лабораторных работ, а также самоподготовки студентов.	Знать: - этапы производства программного продукта; - методы и средства тестирования программ; - способы обеспечения информационной безопасности контента сетевых ресурсов жизненного цикла программного обеспечения; Качество программного обеспечения; Технология вычислительных систем; Системное администрирование; Системная интеграция; Основы программной инженерии; Верификация и испытания программного обеспечения; Встроенные системы; Распределенные системы; Управление	Уметь: криптографические методы защиты информации; протоколы взаимной аутентификации и объектов сетей; методы организации систем защиты информации. методы организации систем защиты информации. .	Владеть: **с техническими средствами разведки, защиты информации и противодействия коммерческой разведке;** **законодательными мерами по защите информации;** методами охраны зданий, помещений, оборудования, документации и персонала в обычных и экстремальных ситуациях, проведения охранных мероприятий в том числе с использованием соответствующих технических средств;

		безопасностью ИТ; в, основные теги и атрибуты; - основные примеры работы с фреймами в HTML-документах;		

7.3 Типовые контрольные задания или иные материалы

Примерный перечень контрольных вопросов и заданий для самостоятельной работы

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 конфиденциаль ных документов, его организационное и технологическое отличие от контроля открытых документов.
3. Классифицировать состав бумажных и технических носителей информа- ции, 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 исполни телей с конфиденциальными документами.
7. Проанализировать пути использования существующих средств копирова- ния и тиражирования документов для изготовления экземпляров и копий кон фиденциальных документов.
8. Обосновать необходимость реквизитов, указываемых на лицевой и обо- ротной 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 в дела 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, егламентировав способы обеспечения их сохранности при упаковке и транспортировке.

Вопросы к экзамену

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 несанкционирован-ного 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 - 50% и промежуточного контроля - 50%.

Текущий контроль по дисциплине включает:

- посещение занятий - 30 баллов,
- участие на практических занятиях - __ баллов,
- выполнение лабораторных заданий – 20 баллов,
- выполнение домашних (аудиторных) контрольных работ - 50 баллов.

Промежуточный контроль по дисциплине включает:

- устный опрос - 50 баллов,
- письменная контрольная работа - 50 баллов,
- тестирование - ___ баллов.

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

а) основная литература:

1. В. П. Мельников, С. А. Клейменов, А. М. Петраков Информационная безопасность и защита информации. 6-е издание. Издательство – 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.: Издателъско-торговый дом «Русская Редакция», 2003. — 704 стр
3. Кузнецов Игорь Николаевич, Информация: сбор, защита, анализ. Учебник по информационно-аналитической работе".. М., ., 2012-150 с.
4. Савченко Е. Кто, как и зачем следит за вами через интернет Из-во. Мир. М., 2012-100с.
5. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности. 2-е изд. М.,.2014-130 с
6. Бауэр Ф. Расшифрованные секреты. Методы и принципы криптологии. Из-во. Мир. М., 2007-550 с.

7. Мазаник С. Безопасность компьютера: защита от сбоев, вирусов и неисправностей.. Мир. М., 2007-256 сМельников В. П., Информационная безопасность и зашита информации: учеб. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков.-М.: Академия, 2011.
8. Тарасов М. А., Электронное правительство и информационная безопасность: учеб. пособие М.: ГАЛАРТ, 2011.
9. Бачило И. Л., Информационное право: учебник М.: Юрайт// ЭБС ЛАНЬ, 2011.
10. Шаньгин В. Ф., Защита информации в компьютерных системах и сетях М.:"ДМК Пресс", 2012.
11. 9. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации. Москва ИНФРА-М, 2001
12. Источники:
13. Закон Российской Федерации от 11.03.1992 № 2487-1 «О частной детективной и охранной деятельности» // Российская газета. – 1992. – № 100.
14. Дополнительная литература:
15. Ковалева Н. Н., Информационное право России: учеб. пособие М.: Дашков и К, 2007
16. Ищейнов В. Я., Мецатунян М. В., Защита конфиденциальной информации: учеб. пособие для вузов/ В. Я. Ищейнов В. Я., М. В. Мецатунян. - М.: ФОРУМ, 2009
17. 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
18. Шаньгин В. Ф Защита компьютерной информации. Эффективные методы и средства.: учебное пособие ДМК Пресс, 2010.
19. Компьютерные сети. 4-е изд. Э.Таненбаум. – СПб.: Питер, 2003. – 992 с.
20. Кучерявский С.В., Суранов А.Я. Основы сетевых технологий. Барнаул: Изд-во Алтайского университета, 2004.
21. Блэк У. Интернет: протоколы безопасности. Учебный курс. СПб.: Питер, 2001.

б) Дополнительная

22. В.Олифер, Н.Олифер. Компьютерные сети. Принципы, технологии, протоколы - СПб: "Питер", 2003.
23. 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.
24. М.А.Мамаев. Телекоммуникационные технологии: Сети TCP/IP. Учебное пособие - Владивосток: Изд-во ВГУЭиС, 1999.
25. Компьютерные системы и сети: Учеб. пособие для вузов/ Под ред. В. П. Косарева, Л. В. Еремина.- М. : Финансы и статистика, 1999.
26. Голдовский И. Безопасность платежей в Интернете. СПб.: Питер, 2001.

27. Крейн Д. и др. Ajax в действии. М.: Вильямс, 2006.
28. Мельников Д.А. Информационные процессы в компьютерных .сетях. Протоколы, стандарты, интерфейсы, модели: М: КУДИЦ-ОБРАЗ, 2001, 256 с.
29. Романец Ю.В.,Тимофеев П.А.,Шаньгин В.Ф. Защита информации в компьютерных .системах и сетях. Изд. 2-е,перераб.,доп. М: Радио и связь, 2001, 376 с.
30. Зегжда Д.П.,Ивашко А.М. Основы безопасности информационных систем. М: Горячая линия-Телеком, 2000, 452 с.

В) Программное обеспечение и Итернет –ресурсы.

Шифр простой постановки, транспозиция, Шифр Виженера и его ваианты, шифр с автоключем, .взлом на Delphi..

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

При освоении дисциплины для выполнения лабораторных работ необходимы персональные компьютеры с набором программного обеспечения: Adobe Photoshop, пакет Denwer-2, web-браузер. Компьютерный класс без доступа в Интернет (автономном режиме). В учебном процессе для освоения дисциплины «Основы Web-программирования» используются следующие технические средства: - компьютеры оборудование. У каждого студента имеются электронные книги.

10. Методические указания для обучающихся по освоению дисциплины.

При решении лабораторных заданий программистский подход непременно должен присутствовать (без него решение не будет полноценным), однако, он не должен заслонять сугубо математические (доказательство и др.) и алгоритмические (построение, оптимизация, верификация и др.) аспекты.

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

При осуществлении образовательного процесса студентами и профессорско-преподавательским составом используются следующее программное обеспечение: Microsoft Visual Studio Express, Microsoft Windows, Ubuntu Linux, Skype. Также студентам предоставляется доступ к российским и международным электронным библиотекам через компьютеры университета.

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

Имеется необходимая литература в библиотеке, медиапроектор и компьютер для проведения лекций-презентаций.

Лабораторные занятия проводятся в компьютерных классах с необходимым программным обеспечением.

Вся основная литература предоставляется студенту в электронном формате.