МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
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 бакалавриата
02.03.02 - Фундаментальная информатика и информационные технологии

Направленность (профиль) подготовки:
Информатика и компьютерные науки

Форма обучения:
очная

Статус дисциплины: входит в часть,
формируемую участниками образовательных отношений

Махачкала, 2022

Рабочая программа дисциплины " Информационная безопасность и защита информации"составлена в 2022 году в соответствии с требованиями ФГОС ВО по направлению подготовки 02.03.02 - Фундаментальная информатика и информационные технологии (уровень бакалавриата).
Приказ №808 Минобрнауки России от 23 августа 2017 г.
.

Разработчик (и): кафедра дискретной математики и информатики, Алибеков Байрамбек Исаевич, д.т.н. по специальности 05.13.18 – «Математическое моделирование, численные методы и комплексы программ» , проф.

Рабочая программа дисциплины одобрена:
на заседании кафедры дискретной математики и информатики от 28 февраля 2022 г., протокол № 6;

зав. кафедрой: _____Магомедов А.М.
и
на заседании Методической комиссии факультета математики и компьютерных наук от 24 марта 2022 г, протокол № 4;

председатель:_____М.К. Ризаев.

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

Начальник УМУ _____ГасангаджиеваА.Г.
(подпись)

Аннотация рабочей программы дисциплины

Дисциплина “**Информационная безопасность и защита информации**” входит в часть, формируемую участниками образовательных отношений 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.

Содержание дисциплины охватывает круг базовых для информационной безопасности и защиты информации вопросов, относящихся общим проблемам:

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.

Дисциплина способствует формированию следующих компетенций выпускника:

общепрофессиональны –(ОПК-5),;профессиональных – *ПК-4*.Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: лекции, лабораторные занятия.

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости: в форме 3-х коллоквиумов и итогового экзамена в конце семестра.

Объем дисциплины составляет 3 зачетных единиц(108 ч.),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						
		Всего	Лекции	Лабораторные занятия	Практические занятия	КСР	консультации		
8	108	48	24	24	0			24	36

1. Цели освоения дисциплины

Целями освоения 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.

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.

2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина “Информационная безопасность и защита информации входит в *часть, формируемую участниками образовательной программы бакалавриата* по направлению 02.03.02 - Фундаментальная информатика и информационные технологии.

Данная дисциплина направлена на изучение системы законодательных и подзаконных актов, составляющих правовую базу защиты информации государством, учреждениями и гражданами, а также принципов и требований к организации конфиденциального делопроизводства и иных защитных мероприятий.

Она направлена также на 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.

Для полноценного усвоения учебного материала по дисциплине "Информационнаябезопасность и защита информации" студентам необходимо иметь прочные знания потехнологии программирования, теории вычислительных сетей, информационнымтехнологиям.

.Для успешного освоения данной дисциплины студенты уже должны освоить курсы по отраслям права (конституционное, административное, гражданское, трудовое), в которых будет дана детальная характеристика базового российского законодательства; а также курсы «»Документоведение» и «Организация и технология ДОУ» для изучения вопросов, связанных с организацией и ведением конфиденциального делопроизводства.

Освоение дисциплине "Информационная безопасность и защита информации" студентам необходимо как предшествующее для изучения других дисциплин, связанных с системами управления базами данных, технологии сети Интернет, так и выполнения других работ, связанных с информационной технологией: Анализ бизнес-требований, Электронная коммерция, Экономика программной инженерии, Сопровождение программного обеспечения, Процессы 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 информационными коммуникациями.

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

Код и наименование компетенции из	**Код и наименование индикатора достижения**	**Планируемые результаты обучения**	Процедура освоения

ОПОП	**компетенций** *(в соответствии с ОПОП*		
ОПК-5. Способен инсталлировать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности	ОПК-5.1. Знает методику установки и администрирования информационных систем и баз данных. Знаком с содержанием Единого реестра российских программ.	Знает: - основные понятия, используемые при изучении ОС (ресурсы компьютера, процесс, поток, задача, виртуальная память, файловая система, ввод-вывод, интерфейс, безопасность, администрирование и другие) Умеет: работать с ОС как в графическом многооконном режиме, так и в режиме командной строки (консоли); Владеет: работы в современных операционных системах, средах и оболочках: :	Устный опрос, письменный опрос; … Конспектирование и проработка лекционного материала. Участие в лабораторных занятиях. Самостоятельная работа.
	ОПК-5.2. Умеет реализовывать техническое сопровождение информационных систем и баз данных.	Знает: Типовые архитектуры сетевых операционных систем; Умеет: применять методики оценки уязвимости в информационно-телекоммуникационных сетях Владеет:	

		способностью брать на себя ответственность за результаты работы по разработке программных средств	
	ОПК-5.3. Имеет практические навыки установки и инсталляции программных комплексов, применения основ сетевых технологий. Технологии баз данных	Знает: основные понятия, функции, состав и принципы работы операционных систем; архитектуры современных операционных систем; Умеет: управлять параметрами загрузки операционной системы; выполнять конфигурирование аппаратных устройств; Владеет методами: управлять дисками и файловыми системами, настраивать сетевые параметры.	
…	…	…	…
ПК-4. Способность применять в профессиональной деятельности современные языки программирования и методы параллельной	ПК-4.1. Знает современные языки программирования и методы параллельной обработки данных. Знаком с содержанием Единого Реестра	Знает: современные методы и средства в информационно-телекоммуникационных системах Умеет: работать с ОС как в графическом	Устный опрос, письменный опрос Наблюдение и участие в выполнении упражнений на лабораторных занятиях, самостоятельное. Конспектирование лекций и изучение

обработки данных, операционные системы, электронные библиотеки и пакеты программ, сетевые технологии.	Российских программ для электронных вычислительных машин и баз данных.	многооконном режиме, так и в режиме командной строки (консоли); Владеет: работы в современных операционных системах, средах и оболочках.	решенных примеров. Лабораторные и самостоятельные занятия.
	ПК-4.2. Умеет реализовывать численные методы решения прикладных задач в профессиональной сфере деятельности, пакеты программного обеспечения, операционные системы, электронные библиотеки, сетевые технологии.	Знать: основные подсистемы ОС Основы управления программными процессами; Умеет: реализовывать простые информационные технологии реализующие методы защиты информации; Владеет: навыками работы в качестве члена группы при проектировании системы	
	ПК-4.3. Имеет практический опыт разработки интеграции информационных систем.	Знает: особенности построения и функционирования семейств операционных систем "Unix" и "Windows"; принципы управления ресурсами в операционной системе; основные задачи	

		администрировани я и способы их выполнения в изучаемых операционных системах; Умеет: управлять учетными записями, настраивать параметры рабочей среды пользователя; управлять дисками и файловыми системами, настраивать сетевые параметры, управлять разделением ресурсов в локальной сети; Владеет: методами управлять разделением ресурсов в локальной сети.	
…	…	…	…

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины

. Объем дисциплины составляет 3 зачетных единиц и экзамень, 108 академических часов.

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.	8	1	2	2	2		
Тема2.Классификация информационных ресурсов, характеристика и основные свойства	8	2	2	2	2		Прием лабораторных работ
Тема 3Классификация и анализ угроз информационной безопасности корпоративным системам.	8	3	2	2	2		Прием лабораторных работ
Тема4. Асимметричные криптосистемы.	8	4	2	2	2		Прием лабораторных работ
Тема 5. Управление ключами.	8	5	2	2	2		
Тема 6Аппаратно-программные решения защиты информации в информационных системах»	8	6	2	2	2		
Итого за модуль 1	36		12	12	12		**Модуль 1**
Модуль 2							
Тема 7 Идентификация и аутентификация объектов сети.	8	9	2	2	2		Прием лабораторных работ
Тема 8Математические методы обеспечения защиты от несанкционирован-ного доступа и конфиденциальности	8	10	2	2	2		Прием лабораторных работ
Тема 9. Криптография и криптоанализ в авторизации, аутентификации и в обмене информации	8	12	2		2		
Тема 10. Средства антивирусной защиты	8	13	2	2	2		Прием лабораторных работ
Тема 11. Архитектура системы защиты информации).	8	14	2	2	2		Прием лабораторных работ
Тема 12. . Информационная	8	15	2	2	2		Прием

безопасность в глобальном информационном простран-стве Интернет. Безопасная интеграция в Интернет. Программные и технологические решения							лабораторных работ
Итого **Итого за модуль 2**	36		12	12	12		**Модуль 2**
Подготовка к экзамену	36				36		Экзамен
Итого за 8 семестр:	108		24	24	24		36

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

4.3.1.Содержание лекционных занятий п дисциплине

Модуль1.

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

Лекция2. Классификация информационных ресурсов, характеристика и основные свойства. Информационные ресурсы в современных условиях, требования к ним, надежность (достоверность) информации и защиты от несанкционированного доступа.

Лекция 3. . Классификация и анализ угроз информационной безопасности корпоративным системам. Уровни защиты информации: правовой; организационный; аппаратно-программный; криптографический

Лекция 4. Классификация криптографических методов. Традиционные (симметричные) криптосистемы. Блоковые и поточные шифры. Стойкость криптосистем. Американский стандарт шифрования данных DES. Отечественный стандарт криптографической защиты ГОСТ 28147-89.

Лекция 3. 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

Лекция 6. «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

Лекция 8.Инфраструктура открытых ключей. Цифровые сертификаты. Электронная цифровая подпись (ЭЦП). Однонаправленная хэш-функция.

Модуль 2

Лекция 7. Идентификация и аутентификация объектов сети. Идентификация и подтверждение подлинности пользователей сети.

Лекция 8.«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

Лекция 9.Межсетевое экранирование. Принципы построения и функционирования межсетевых экранов (МЭ). Классификация МЭ. Особенности межсетевого экранирования на различных уровнях модели OSI

Лекция 10.«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 11. Средства антивирусной защиты. Классификация вирусов и средств защиты. Виды антивирусных программных продуктов. Характеристика наиболее популярных антивирусных пакетов.

Лекция я 12. «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

4.3.2. Содержание лабораторны занятий по дисциплине.

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

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		
№№ и названия разделов и тем	Цель и содержание лабораторной работы	Результаты лабраторной 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 пароляЗащита на уровне пользователя. Создать и изменеть 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 шифрование
Лабораторная работа 4.. «Основы криптографической защиты информации. Асимметричные алгоритмы».	Асимметричные криптосистемы Схема шифрования Эль Гамаля. Алгоритм Диффи-Хелмана. Криптосистема шифрования данных RSA	Процесс шифрование
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 ключем.	Процесс шифрование
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.
Лабораторная работа 7. Создания файлов для хранения сведений о пользователе	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 о пользователе на сервере Извлечение сведений о пользователе из набора данных

	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.	
Лабораторная работа 8. Проверка наличия поддержки дополнительныхвозможностей	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
Модуль2		
Лабораторная работа 9. Аутентификация и авторизация пользователей	Войдите на сервер как администратор. . Выберитеизменю Start (Пуск) пункт Administrative Tools\Computer Management (Ад- министрирование\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, выде- ленную полужирным шрифтом в HTML-коде), а если Visual C# — то следующий эле- мент необходимо добавить целиком:Добавьте к коду начальнойWeb-формы проекта следующее HTML-определение таблицы Переключите окно формы в режим Design и добавьте к объекту	Web-форма

	кода начальной Web- формы следующие строки	
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 быстро создавать элементы спис- ка путем копирования-вставки соответствующего HTML-кода. Вот HTML-код, опре- деляющий DropDownList и элементы его списка:	СозданиеWeb-формы

5. Образовательные технологии.

Методика преподавания дисциплины «Информационная безопасность и защита информации» строится на сочетании лекционных и лабораторных занятий с групповыми и индивидуальными консультациями. Лабораторные занятия проводятся по лекционным темам дисциплины. Но в любом случае студенты должны овладеть способами приобретения знаний о специальности и научиться логически мыслить.

Для понимания и усвоения студентами материала по дисциплине «Информационная безопасность и защита информации» целесообразно следовать следующим требованиям:

– создавать для обучения условия и проблемные ситуации, когда студенты могли бы воспользоваться своим жизненным опытом и оценить приобретенными ими знаниями по данной дисциплине;

– стимулировать студентов к поиску причинно-следственных связей, их упорядочиванию и систематизации;
– помогать студентам формировать навыки в систематическом исследовании обсуждаемого материала;
– прививать интерес к научному анализу и обобщению.
Изучение тем лабораторных занятий необходимо начинать с определения базовых терминов и понятий, являющихся основой для понимания правовых основ защиты информации. Важно раскрыть содержание и объем дефиниций, выделить их существенные признаки и связи с другими понятиями, роль исторических предпосылок в формировании нормативно-правовой базы защиты информации, усиление роли правовой защиты информации в нарастающем потоке информационных ресурсов, увеличения значимости документа в системе рыночной экономики.
Необходимо готовить конспект выступления на лабораторныхзанятия занятях, внимательно прочитать этот конспект (план ответа), выделить исследуемый вопрос и аспекты раскрывающие его. Ответив на вопросы, выносимые на обсуждение, необходимо убедиться в правильности полученных знаний.

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
Брюс Шнайр прикладная криптография 2-издание. Протоколы, алгоритмы и исходные тексты на языке С.(Электронном варианте).	
Криптографические протоколы.	Элементы протоколов.. Введение в протоколы. Передача информации с использованием симметричной криптографии. Однонаправленые фукции
Криптографические протоколы.	Однонаправленные хэш-функции Передача информации сиспользованием криптографии с открытыми ключами. Цифровые подписи .Цифровые подписи . и шифрование. Генерация случайных и псевдослучайных последовательностей
Основные протоколы	Обмен ключами. Удоствоверение подлинности.формальный анализ протоколов проверки подлинности иобмена ключами. Разделение секрета. Совместное использование секрета. Криптографическая защита баз данных
Промежуточные протоколы	Служба меток времени. Подсознательный канал. Неотрицаемые цифровые подписи.подписи уполномоченного свидетеля. Подписи по доверенности. Групповые подписи. Подписи с

	обнаружением подделки
Промежуточные протоколы	Вычисления с зашифрованными данными. Вручение битов. Побрасывание «честной » монеты. Мысленный покер. Однонаправленные сумматоры. Раскрытие секретов «все или ничего» Условие вручение ключей.
Развитые протоколы.	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
Эзоерические протоколы	Безопасные выборы. Безопасные вычисления с несколькими участниками. Анонимная широковещательная передача сообщений. Электронные наличные.
Длина ключа	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?
Управление ключами	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.
Типы алгоритмов и криптографические режимы.	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.
Математические основы	Теория инормации. Теория сложности. Теория чисел.
	Разложение на множители. Генерации прстых чисел. Дискретные логорифмы и конечное поле
Стандарт шфрование данных DES	Описание JgbcfybtDES.безопасность DES. Варианты DES. Насколько безопасен сегодняDES.

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

7.1 Типовые контрольные задания

7.1.1. 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.
7. Проанализировать содержание понятия разрешительной системы доступа персонала к конфиденциальным сведениям фирмы.
8. Проанализировать состав показателей (граф и зон) перечня конфиденциальных сведений фирмы, обосновать целевое назначение показателей и их взаимосвязь.
9. Регламентировать в виде фрагмента инструкции порядок доступа персонала к электронным конфиденциальным документам фирмы.
10. Обосновать критерии выделения конфиденциальных документов из общего потока поступающих документов.

7.2. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций. (процентное соотношение баллов при контроле)

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ
контрольных работ
Контрольные работы выполняются студентами в течение изучения курса и представляют собой, так называемый, текущий контроль знаний студентов. Они имеют большой диапазон различных видов, что в совокупности дает основание для определения объективной итоговой оценки по дисциплине в целом.
Текущий контроль знаний студентов включает :
• устный или письменный блиц-опрос студентов по прочитанной лекции (10 мин.), ответы на вопросы для всех студентов,
• контрольная работа по практическому занятию,
• коллоквиум - опрос студентов индивидуальный или в виде дискуссии, собеседование по комплексу сообщаемых заранее проблем (вопросов).

Оценка по результатам практического занятия поставляется студенту, выступившему с докладом или сообщением. Оценка проставляется также студентам после отработки ими пропущенных практических занятий.
Устный или письменный блиц-опрос студентов проводится, как правило, по предыдущей прочитанной лекции. Студентам задается 5 вопросов, на которые они отвечают без использования каких-либо материалов. Работа каждого студента оценивается по шестибальной шкале (от 0 до 5).
На каждом третьем практическом занятии студентам дается письменная контрольная работа по изученным вопросам. Каждый студент получает задание (вопрос), на которое он должен письменно ответить. Работа оценивается также по шестибальной шкале.
В конце изучения дисциплины может проводиться проблемная итоговая контрольная работа, результаты которой в совокупности с другими оценками текущего контроля могут рассматриваться как письменный экзамен.

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

К экзамену не допускаются студенты, не выполнившие учебную программу (не выполнившие практические работы, не выполнившие практические задания, выдаваемые преподавателем).

Контроль качества освоения дисциплины

1. Текущий контроль**.**

Проводится по каждой учебной единице в форме проверки домашнего задания.

2. Рубежный контроль.

Проводится 2 модуля в форме контрольных работ с рейтинговой оценкой от 0 до 100 баллов.

3. Итоговый контроль**.**

Проводится в форме зачета.

Общий результат выводится как интегральная оценка, складывающая из текущего контроля - 50% и промежуточного контроля - 50%.

Текущий контроль по дисциплине включает:

- посещение занятий - 30 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,

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

1. . а) адрес сайта курса
2. Интернет-адрес сайта. eLIBRARY.RU[Электронный ресурс]: электронная библиотека / Науч. электрон. б-ка. — Москва, 1999 – Режим доступа: http://elibrary.ru/defaultx.asp (дата обращения: 01.11.2019). – Яз. рус., англ.
3. Электронный каталог НБ ДГУ[Электронный ресурс]: база данных содержит сведения о всех видах лит, поступающих в фонд НБ ДГУ/Дагестанский гос. ун-т. – Махачкала, 2010 – Режим доступа: http://elib.dgu.ru, свободный Список основной литературы

4. Галатенко, Владимир Антонович.и Основы информационной безопасности : учеб. пособие для студентов вузов, обуч. по специальности 351400 "Прикл. информ." / Галатенко, Владимир Антонович. - 4-е изд. - М. : Изд-во Интернет-Ун-та Информ. Технологий: БИНОМ. Лаб. знаний, 2016, 2008, 2006. - 205 с. - (Основы информационных технологий). - Рекомендовано УМО. - ISBN 978-5-94774-821-5 : 230-00.**Местонахождение:** Университетская библиотека ONLINE, IPRbooks **URL:**http://biblioclub.ru/index.php?page=book&id=233063, http://www.iprbookshop.ru/52209.html

5. **Мельников, Владимир Павлович.** Информационная безопасность и защита информации : учеб. пособие для студентов вузов, обуч. по специальности "Информ. системы и технологии" / Мельников, Владимир Павлович, С. А. Клейменов ; под ред. С.А.Клейменова. - 5-е изд., стер. - М. : Академия, 2011, 2010. - 330,[6] с. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Допущено УМО. - ISBN 978-5-7695-7738-3 : 401-06.

Местонахождение: Научная библиотека ДГУ

6. **Бабаш, Александр Владимирович.** Информационная безопасность : лаб. практикум; учеб. пособие / Бабаш, Александр Владимирович, Е. К. Баранов. - 2-е изд., стер. - И. : Кнорус, 2016, 2011. - 306-00.

Местонахождение: Университетская библиотека ONLINE **URL:** http://biblioclub.ru/index.php?page=book&id=90539

7. **Сергеева, Ю.С.**

Защита информации. : Конспект лекций. Учебное пособие / Ю. С. Сергеева ; Сергеева Ю. С. - М. : А-Приор, 2011. - 128. - (Конспект лекций). - ISBN 978-5-384-00397-7.

Местонахождение: Российская государственная библиотека (РГБ) **URL:** http://нэб.рф/catalog/000199_000009_006559182/

8. Прохорова, О.В. **Информационнаябезопасность** и **защитаинформации** : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-9585-0603-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=438331

9. Инструментальный контроль и **защитаинформации** : учебное пособие / Н.А. Свинарев, О.В. Ланкин, А.П. Данилкин и др. ; Министерство образования и науки РФ, ФГБОУ ВПО «Воронежский государственный университет инженерных технологий». - Воронеж : Воронежский государственный университет инженерных технологий, 2013. - 192 с. : табл., ил. - Библиогр. в кн. - ISBN 978-5-00032-018-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=255905

10. Бурькова, Е.В. Физическая **защита** объектов информатизации : учебное пособие / Е.В. Бурькова ; Министерство образования и науки Российской Федерации, Оренбургский Государственный Университет, Кафедра вычислительной техники и **защиты** **информации**. - Оренбург : Оренбургский государственный университет, 2017. - 158 с. : табл., схем. - Библиогр. в кн. - ISBN 978-5-7410-1697-8 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=481730

Дпольнительная

1. Алешников С.И. Математические методы защиты информации. Часть 4. Вычислительный практикум по эллиптическим кривым и криптографии на эллиптических кривых [Электронный ресурс] : практическое пособие / С.И. Алешников, Ю.Ф. Болтнев. — Электрон. текстовые данные. — Калининград: Балтийский федеральный университет им. Иммануила Канта, 2007. — 58 с. — 978-588874-803-9. — Режим доступа: http://www.iprbookshop.ru/23795.html

2. Алешников С.И. Математические методы защиты информации. Часть 5. Методы алгебраических кривых [Электронный ресурс] : учебное пособие / С.И. Алешников, Е.С. Алексеенко. — Электрон. текстовые данные. — Калининград: Балтийский федеральный университет им. Иммануила Канта, 2010. — 158 с. — 9785-9971-0073-5. — Режим доступа: http://www.iprbookshop.ru/23796.html

3. Алешников С.И. Математические методы защиты информации. Часть 3. Вычислительный практикум по числовым полям и криптографии в квадратичных полях [Электронный ресурс] : практическое пособие / С.И. Алешников, Е.В. Козьминых. — Электрон. текстовые данные. — Калининград: Балтийский федеральный университет им. Иммануила Канта, 2006. — 97 с. — 588874-689-4. — Режим доступа: http://www.iprbookshop.ru/23851.html

4. Бескид П.П. Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации [Электронный ресурс] : учебное пособие / П.П. Бескид, Т.М. Тагарникова. — Электрон. текстовые данные. — СПб. : Российский государственный гидрометеорологический университет, 2010. — 104 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/17926.html

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

1) **window.edu.ru**›resource/482/57482/files/infbez.pdf
2)**habr.com**›company/vps_house/blog/343110/
spravochnick.ru›informacionnaya_bezopasnost…i…

3)**intuit.ru**›studies/courses/697/553/lecture/12442

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: MicrosoftVisualStudioExpress, MicrosoftWindows, UbuntuLinux, Skype. Также студентам предоставляется доступ к российским и международным электронным библиотекам через компьютеры университета.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.

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.