МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет Информатики и Информационных Технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Криптографические методы защиты информации

Кафедра Информатики и информационных технологий

Образовательная программа
Информационная безопасность

10.03.01 Профиль подготовки

Безопасность компьютерных систем

Уровень высшего образования

Бакалавриат

Форма обучения

очная

Статус дисциплины: базовая

Махачкала, 2020

Рабочая программа дисциплины «Криптографические методы защиты информации» составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 – Информационная безопасность, уровень подготовки: бакалавриат, утвержденного приказом Минобрнауки РФ от 1 декабря 2016 г. №1515.

Составитель: Ахмедова Написат Мурадовна, старший преподаватель кафедры информатики и информационных технологий

Рабочая программа дисциплины одобрена:
на заседании кафедры ИиИТ эт «13» _03_2020г., протокол № 8

Зав. кафедрой _____ Ахмедов С.А.
(подпись)

на заседании Методической комиссии факультета ИиИТ

от от «_12_» _03_2020__г., протокол №_8_.

председатель _____ Ахмедова З.Х.

Рабочая программа дисциплины согласована с учебно-методическим управлением «26» 03 2020 г. _____
(подпись)

Аннотация рабочей программы дисциплины

Дисциплина ***Криптографические методы защиты информации*** входит в базовую часть образовательной программы *бакалавриата,* по направлению 10.03.01 Информационная безопасность

Дисциплина реализуется на факультете ИиИТ кафедрой ИиИТ..

Содержание дисциплины охватывает круг вопросов, связанных с защитой информации путем математических преобразований с помощью криптографических алгоритмов.

Дисциплина нацелена на формирование следующих компетенций выпускника: общекультурных – ОК-5, общепрофессиональных – ОПК-2, ОПК-7 профессиональных – ПК-1,ПК-2.

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

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости в форме - *контрольная работа, коллоквиум и пр.* и промежуточный контроль в форме - *экзамена*.

Объем дисциплины 5 зачетных единиц, в том числе 180 академических часов по видам учебных занятий

Семестр	Учебные занятия							Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен
	в том числе:							
	всего	Контактная работа обучающихся с преподавателем					СРС, в том числе экзамен	
		из них						
		Лекции	Лабораторные занятия	Практические занятия	КСР	консультации		
7	180	20	36	18			106	экзамен

1. Цели освоения дисциплины

Целью освоения дисциплины ***Криптографические методы защиты информации*** является изучение основных математических подходов к решению задач компьютерной безопасности и, прежде всего, к построению современных криптографических алгоритмов.

2.Место дисциплины в структуре ОПОП бакалавриата

Дисциплина ***Криптографические методы защиты информации*** входит в базовую часть образовательной программы *бакалавриата,* по направлению 10.03.01 Информационная безопасность

Для освоения дисциплины необходимо знание курсов: «Математический анализ», «Алгебра и теория чисел», «Теория вероятности и математическая статистика», «Информатика», «Языки программирования», «Теория информации», «Теоретико-числовые методы криптографии». В результате изучения данной дисциплины студенты освоят непростые математические принципы организации криптографической защиты информации, передаваемой и обрабатываемой техническими средствами, что является неотъемлемой составляющей подготовки учащихся по направлению 10.03.01 Информационная безопасность. Курс необходим для дисциплин компьютерной безопасности.

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

Код компетенции из ФГОС ВО	Наименование компетенции из ФГОС ВО	Планируемые результаты обучения
ОК-5	способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Знать: место и роль информационной безопасности в системе национальной безопасности РФ; социальные ценности общества и их связь с социальной значимостью своей будущей профессии. Уметь: осознавать социальную значимость своей профессии, анализировать и оценивать социальную информацию, планировать и осуществлять свою деятельность с учетом результатов этого анализа. Владеть: пониманием социологического аспекта профессионализации и высокой мотивацией к выполнению профессиональной деятельности.
ОПК-2	способностью применять соответствующий математический аппарат для решения профессиональных задач	Знает: математические основы современной криптографии; модели шифров и математические методы их исследования; Умеет: применять математические методы криптографической защиты информации, Владеет: навыками математического моделирования в криптографии.
ОПК-7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Знает: место криптографии в задаче информационной безопасности и построения защищенных информационных систем Умеет: ориентироваться в современной системе источников информации; видеть и формулировать проблему защиты информации; Использовать криптографические методы при организации работ по защите информации Владеет: навыками самостоятельной исследовательской работы;
ПК-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и	Знать: основные задачи и понятия криптографии; Уметь: использовать программные и аппаратные средства персонального компьютера; пользоваться программными

	технических средств защиты информации	средствами, реализующими основные криптографические функции - системы публичных ключей, цифровую подпись, разделение доступа; Владеть: навыками использования инструментов криптографической защиты информации;
ПК-2	способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	**знать**: основные задачи и понятия криптографии; требования к шифрам и основные характеристики шифров; принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах; **уметь**: выполнять шифрование и дешифрование текста с помощью различных криптоалгоритмов, осуществлять программирование используемых алгоритмов, проводить строгую математическую проверку стойкости шифра; **владеть**: способами построения типовых криптографических алгоритмов

4. Объем, структура и содержание дисциплины.

Объем дисциплины составляет 5 зачетных единиц, 180 академических часов.

Структура дисциплины.

№ п/п	Разделы и темы дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Самостоятельная работа	Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные занятия	Контроль самост. раб.		
	Модуль 1. Простые шифры								
1	Введение в криптографию			2				6	устный и письменный опросы
2	Шифр Цезаря. Шифр простой замены.			2	2	4		6	устный и письменный опросы, лабораторные работы.
3	Шифр Виженера. Частотный анализ.			2	2	4		6	устный и письменный опросы, лабораторные работы.
	Итого по модулю 1:			6	4	8		18	
	Модуль 2. *Шифрование с закрытым ключом*								
1	Классификация шифров перестановки. Примеры шифров перестановки и их криптоанализ			2	2	4		10	устный и письменный опросы, лабораторные работы.
2	Шифры гаммирования. Композиции шифров			2	2	4		10	устный и письменный опросы, лабораторные работы.
	Итого по модулю 2:			4	4	8		20	
	Модуль3 Блочные шифры								
	Сеть Фейстеля			2	2	4		4	устный и письменный опросы, лабораторные работы.

	DES/3DES			2	2	4		4	устный и письменный опросы, лабораторные работы.
	AES			2	2	4		4	устный и письменный опросы, лабораторные работы.
	Итого по модулю 3:			6	6	12		12	
	Модуль 4. Шифрование с открытым ключом								
	АЛГОРИТМ Диффи-Хелмана			2	2	4		10	устный и письменный опросы, лабораторные работы.
	RSA			2	2	4		10	устный и письменный опросы, лабораторные работы.
	Итого по модулю 4:			4	4	8		20	
	Модуль5							36	экзамен
	ИТОГО:			20	18	36			

Содержание дисциплины, структурированное по темам (разделам).

Содержание лекционных занятий по дисциплине.

Модуль1. Криптография.

Основные понятия криптографии. Введение в криптографию. Криптографические атаки. Криптографический протокол.

Шифр Цезаря. Методы замены Модуль

2. Шифры с закрытым ключом.

Простейшие методы шифрования с закрытым ключом.

Методы перестановки. 2.3.Понятие композиционного шифра.

Модуль 3. Алгоритмы шифрования DES и AES. Хеширование.

Принципы построения блочных шифров с закрытым ключом. Режимы работы блочных шифров. Сеть Фейштеля.

Алгоритмы шифрования DES и AES. Общие сведения. Шифрование и расшифрование.

Криптографические хеш-функции. Понятие хеш-функции. Обзор алгоритмов формирования хеш-функций.

Модуль 4. Шифры с открытым ключом. Алгоритм RSA. Электронная цифровая подпись. Криптостойкость и имитостойкость шифров.

Шифры с открытым ключом. Односторонние функции. Использование ассиметричных алгоритмов для шифрования.

Алгоритм RSA. Основные сведения. Пример вычислений по алгоритму. Практическое использование алгоритма RSA.

Электронная цифровая подпись

Криптостойкость и имитостойкость шифров.

Содержание лабораторно-практических занятий по дисциплине.

Модуль 1.

1. Шифрование с закрытым ключом незнакомого теста.
2. Программная реализация шифра Цезаря.
3. Одноалфавитная замена. Пропорциональные шифры.
4. Многоалфавитные подстановки, методы гаммирования.
5. Методы перестановки. Понятие композиционного шифра.
6. Программная реализация шифра Вижинера.
7. Поточные шифры.
8. DES-шифрование.
9. Использование алгоритма хеширования для сокрытия содержимого файла.
10. Использование алгоритма хеширования для подтверждения неизменности

файла.

11. Base-64.
12. Кодирование бинарных зашифрованных файлов в base 64.
13. Создание цифровых сертификатов.
14. Применение электронной цифровой подписи для проверки авторства.
15. Применение электронной цифровой подписи для проверки неизменности файла.
16. Безопасное хранение файлов с применением криптоконтейнеров.
17. Скрытия факта передачи шифрованного текста (стеганография).
18. Создание файловой системы с поддержкой прозрачного шифрования….

5. Образовательные технологии

Предусмотрено сочетание традиционных видов учебной активности, таких как конспектирование лекций и контроль усвоения теоретического материала в виде коллоквиумов, так и интерактивных технологий, таких как собеседования, ситуационные игры на выбор методов защиты информации на практических занятиях.

Подготовка студентами докладов по темам, не входящим в план лекций, а также выполнение расчетных работ, позволяют расширить научный кругозор студентов, повысить навык работы с учебной и научной отечественной и зарубежной литературой, развить языковые навыки, повысить математическую подготовку, укрепить междисциплинарные связи, повысить навык программирования.

6. **Учебно-методическое обеспечение самостоятельной работы студентов.**

В соответствии с учебным планом предусмотрен экзамен в седьмом семестре.
Формы контроля: текущий контроль, промежуточный контроль по модулю, итоговый контроль по дисциплине.
Форма текущего контроля – выполнение семестровых заданий. В течение семестра студент выполняет задания, за каждой из которых получает соответствующие баллы. За выполнение задания студент получает определенное количество баллов.
Форма промежуточного контроля – контрольные, коллоквиум.
Форма итогового контроля, определенная учебным планом, - экзамен.

Темы для самостоятельного изучения:

Наименование темы:	Вид работы:	№ занятия	Количество часов
1.Инструментальные средства и библиотеки для реализации криптографических алгоритмов	Изучение функций библиотек GNU MP и GNU Crypto по технической документации	1,2	10
2. Теоретико –числовые методы в криптографии. Вычисления в простых полях и кольцах целых чисел	Изучение разделов дисциплины по учебной литературе, в том числе вопросов, не освещаемых на лекциях: Алгоритмические аспекты поиска больших простых чисел Подготовка к практическим занятиям	3-4	20
3.Система Диффи-Хеллмана, шифр Шамира, шифр Эль - Гамаля (по выбору)	Выполнение расчетного задания в виде компьютерной программы по темам	5-6	10
4.Сложность дискретного логарифмирования и наиболее быстрые алгоритмы.	Изучение разделов дисциплины по учебной литературе, в том числе вопросов, неосвещаемых на лекциях. Подготовка к практическим занятиям	7-8	10
5.Шифр RSA, подпись RSA, шифр Рабина (по выбору)	Выполнение расчетного задания в виде компьютерной программы по темам.	9	10
6.Теория секретных систем Шеннона и современные подходы к теоретико-информационной секретности	Выполнение расчетного задания в виде компьютерной программы по теме: реализация простейших омофонных кодов и их применение для построения идеальной криптосистемы для	10	10

	сообщений, порождаемых источником без памяти с неизвестной статистикой.		

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

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

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

Код компетенции из ФГОС ВО	Наименование компетенции из ФГОС ВО	Планируемые результаты обучения	**Процедура освоения**
ОК-5	способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Знать: место и роль информационной безопасности в системе национальной безопасности РФ; социальные ценности общества и их связь с социальной значимостью своей будущей профессии. Уметь: осознавать социальную значимость своей профессии, анализировать и оценивать социальную информацию, планировать и осуществлять свою деятельность с учетом результатов этого анализа. Владеть: пониманием социологического аспекта профессионализации и высокой мотивацией к выполнению профессиональной деятельности.	устный и письменный опросы, лабораторные работы.
ОПК-2	способностью применять соответствующий математический аппарат для решения профессиональных задач	Знает: математические основы современной криптографии; модели шифров и математические методы их исследования; Умеет: применять математические методы криптографической защиты информации, Владеет: навыками математического моделирования в криптографии.	устный и письменный опросы, лабораторные работы.
ОПК-7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Знает: место криптографии в задаче информационной безопасности и построения защищенных информационных систем Умеет: ориентироваться в современной системе источников информации; видеть и формулировать проблему защиты информации; Использовать криптографические методы при организации работ по защите информации Владеет: навыками самостоятельной исследовательской работы;	устный и письменный опросы, лабораторные работы.
ПК-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Знать: основные задачи и понятия криптографии; Уметь: использовать программные и аппаратные средства персонального компьютера; пользоваться программными средствами, реализующими основные криптографические функции - системы публичных ключей, цифровую подпись, разделение доступа; Владеть: навыками использования инструментов криптографической	устный и письменный опросы, лабораторные работы.

		защиты информации;	
ПК-2	способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	**знать**: основные задачи и понятия криптографии; требования к шифрам и основные характеристики шифров; принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах; **уметь**: выполнять шифрование и дешифрование текста с помощью различных криптоалгоритмов, осуществлять программирование используемых алгоритмов, проводить строгую математическую проверку стойкости шифра; **владеть**: способами построения типовых криптографических алгоритмов	**устный и письменный опросы, лабораторные работы.**

Типовые контрольные задания

ПЕРЕЧЕНЬ КОНТРОЛЬНЫХ ВОПРОСОВ ДЛЯ ПОДГОТОВКИ К ИТОГОВОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

1. Основные понятия и определения криптографии.
2. Виды криптосистем. Задачи, решаемые методами криптографии.
3. Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений.
4. История криптографии. Основные этапы становления науки криптографии.
5. Классификация шифров замены. Шифр Цезаря. Шифр простой замены. Шифр Плейфера. Полибианский квадрат. Шифр Хилла. Шифр Виженера. Частотный анализ. Тест Казиски.
6. Классификация шифров перестановки. Примеры шифров перестановки и их криптоанализ.
7. Шифры гаммирования. Шифр Вернама. Подходы к его криптоанализу.
8. Композиции шифров. Enigma. Шифр Хейглина.
9. Математическая модель шифра.
10. Атаки и угрозы шифрам.
11. Блочные шифры и их ключевая система. Замены и перестановки.
12. Сеть Файстеля. Шифры DES, ГОСТ 28147-89.
13. Шифр AES
14. Шифр IDEA.
15. Подходы к криптоанализу блочных шифров. Дифференциальный криптоанализ. Линейный криптоанализ.
16. Режимы шифрования.
17. Многократное шифрование. Композиция блочных шифров.
18. Совершенные шифры. Пример совершенного шифра.
19. Энтропийные характеристики шифров. Идеальные шифры.
20. Избыточность языка.
21. Оценка числа ложных ключей и расстояние единственности.
22. Безусловно стойкие и вычислительно стойкие шифры.
23. Псевдослучайные последовательности (ПСП). Характеристики генераторов ПСП (ПСГ). Требования к криптографическим ПСП. Примеры ПСГ и криптографических ПСГ.

24. Поточные шифры. Общая схема поточного шифра. Синхронные и самосинхронизирующиеся шифры.
25. Регистры сдвига с обратной линейной связью (РСЛОС).
26. ПСГ на основе РСЛОС.
27. Шифр A5.
28. Нелинейные регистры сдвига.
29. Шифр RC4.
30. Теория имитостойкости Симмонса. Имитация и подмена сообщения. Характеристики имитостойкости. Совершенная имитостойкость.
31. Коды аутентификации сообщений.
32. Защитные контрольные суммы.
33. Криптографические хэш-функции и требования к ним.
34. Подходы к проектированию хэш-функций.
35. Хэш-функции на основе блочного шифра.
36. Ключевые хэш-функции.
37. Понятие односторонней функции и односторонней функции с "лазейкой". Проблемы факторизации целых чисел и логарифмирования в конечных полях.
38. Криптосистема Диффи-Хэллмана. Пример.
11
39. Криптосистема RSA. Пример.
40. Криптосистема Эль-Гамаля. Пример.
41. Криптосистема Рабина. Пример.
42. Криптосистема Гольдвассер-Микали. Пример.
43. Криптосистема Блюма-Гольдвассер. Пример.
44. Рюкзачные шифры. Криптосистема Меркла-Хэллмана.
45. Понятие электронной цифровой подписи и требования к ней. Атаки и угрозы схемам ЭЦП.
46. Подпись RSA, Эль-Гамаля.
47. Подпись Фиата-Шамира.
48. Подпись Онга-Шнорра-Шамира.
49. Неотрицаемая подпись Шаума-ван-Антверпена.
50. Эллиптическая кривая над конечным полем. Операции на эллиптической кривой. Сумма точек. Кратная точка.
51. Шифр Эль-Гамаля на эллиптической кривой.

ПЕРЕЧЕНЬ ТЕМ РЕФЕРАТОВ

1) Криптография в Древнем мире.
2) Исторические методы стеганографии.
3) Криптография в Средние века и в Новое время.
4) Дисковые шифраторы.
5) Криптография на рубеже 19-20 вв.
6) История отечественной криптографии.
7) Шифрование аналогового сигнала.
8) Клод Шеннон и его вклад в криптографию.
9) Алан Тьюринг и его вклад в криптографию.
10) Лауреаты премии Алана Тьюринга.
11) Первый блочный шифр – Lucifer.
12) Современная стеганография – математические методы.
13) Электронные водяные знаки.
14) Ади Шамир и его вклад в криптографию.
15) Шифрование и аутентификация в современных беспроводных сетях связи.

16)Парольные схемы аутентификации.
17) Одноразовые пароли.
18) Протоколы с нулевым разглашением
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 - _60___% и промежуточного контроля - _40____%.
Текущий контроль по дисциплине включает:
- посещение занятий - 10_ баллов,
- участие на практических занятиях - _10_ баллов,
- выполнение лабораторных заданий - _30 баллов,
- выполнение домашних (аудиторных) контрольных работ - _10 баллов.
Промежуточный контроль по дисциплине включает:
- устный опрос - _10 баллов,
- письменная контрольная работа - _20___баллов,
- тестирование - _10 баллов.

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

а) основная литература:

1) **Иванов, Михаил Александрович.** Криптографические методы защиты информации в компьютерных системах и сетях. - М. : КУДРИЦ-ОБРАЗ, 2001. - 363 с. - ISBN 5-93378-021-9 : 0-0..

2) **Торстейнсон, Питер.** Криптография и безопасность в технологии .NET / пер. с англ. В.Д.Хорева; под ред. С.М.Молявко. - М. : БИНОМ. Лаб. знаний, 2007. - 479 с. : ил. - (Программисту). - Предм. указ.: с. 448-472. - ISBN 978-5-94774-312-8 : 380-00

3) **Кирпичников А.П.** Криптографические методы защиты компьютерной информации [Электронный ресурс] : учебное пособие / А.П. Кирпичников, З.М. Хайбуллина. — Электрон. текстовые данные. — Казань: Казанский национальный исследовательский технологический университет, 2016. — 100 с. — 978-5-7882-2052-9. — Режим доступа: http://www.iprbookshop.ru/79313.html

б) дополнительная литература:

1. **Калмыков И.А.** Криптографические методы защиты информации [Электронный ресурс] : лабораторный практикум / И.А. Калмыков, Д.О. Науменко, Т.А. Гиш. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 109 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/63099.html

2. Практикум по выполнению лабораторных работ по дисциплине Криптографические методы защиты информации [Электронный ресурс] / . — Электрон. текстовые данные. — М. : Московский технический университет связи и информатики, 2015. — 67 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61738.html

3. Учебно-методическое пособие по выполнению курсовой работы по дисциплине Криптографические методы защиты информации [Электронный ресурс] / . — Электрон. текстовые данные. — М. : Московский технический университет связи и информатики, 2015. — 28 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/63335.html

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

1) eLIBRARY.RU [Электронный ресурс]: электронная библиотека / Науч. электрон. б-ка. – – Москва, 1999 – . Режим доступа: http://elibrary.ru/defaultx.asp (дата обращения: 01.02.2020). – Яз. рус., англ.

2) Moodle [Электронный ресурс]: система виртуального обучением: [база данных] / Даг. гос. ун-т. – Махачкала, г. – Доступ из сети ДГУ или, после регистрации из сети ун-та, из

любой точки, имеющей доступ в интернет. – URL: http://moodle.dgu.ru/ (дата обращения: 22.03.2020).
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 (дата обращения: 21.03.2020).
4) Информационный портал по безопасности **SecurityLab.ru**, новости, статьи, обзор уязвимостей, вирусов и мнения аналитиков.

10. Методические указания для обучающихся по освоению дисциплины.

Практические занятия по дисциплине «Криптографические методы защиты информации» служат для получения практических навыков по применению теоретических знаний, полученных студентами на лекциях, для решения конкретных задач в профессиональной сфере специалистов в области защиты информации.
Решения задач фиксируются с помощью реализованных программ на различных языках программирования(Delphi, Pascal, C, C++) .
Для более полного понимания целей, задач и практических результатов теории систем следует: 1) Ознакомиться с дополнительной литературой, особенно с трудами основоположников. 2) Ознакомиться, хотя бы поверхностно, с другими подходами к построению систем (см. доп. литературу). 3) Попытаться в рамках практических и лабораторных занятий самостоятельно и полностью выполнить все задания.

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

Учебная аудитория, оборудованная мультимедиа проектором. Компьютер под управлением операционной системы Windows 7, 8.0, 8.1, имеющий установленный пакет офисных программ MSOffice 2010, 2013 и Microsoft Visual Studio.

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

а) Мультимедийная аудитория - для лекций;
б) Компьютерный класс, оборудованный для проведения практических работ средствами оргтехники, персональными компьютерами, объединенными в сеть с выходом в Интернет – для практических занятий.
Для проведения лекционных занятий требуется аудитория на курс, оборудованная интерактивной доской, мультимедийным проектором с экраном.
Для проведения практических занятий требуется аудитория на группу студентов, оборудованная интерактивной доской, мультимедийным проектором с экраном.
Для проведения практических занятий на ПЭВМ требуется компьютерный класс с установленной на ПЭВМ: 1. Microsoft Office 2. Microsoft Visual Studio.