МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Колледж

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ МДК.02.02. КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

по программе подготовки специалистов среднего звена (ППССЗ) среднего профессионального образования

Специальность:	*10.02.05.Обеспечение информационной безопасности автоматизированных систем*
Обучение:	*по программе базовой подготовки*
Уровень образования, на базе которого осваивается ППССЗ:	*среднее общее образование*
Квалификация:	*техник по защите информации*
Форма обучения:	*очная*

Махачкала - 2022

Рабочая программа дисциплины « Криптографические средства и методы защиты информации» разработана на основе требований ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем по программе базовой подготовки для реализации основной профессиональной образовательной программы СПО на базе основного общегообразования с получением среднего общего образования.

Организация-разработчик: Колледж ДГУ

Разработчики:

Магомедова Карина Камильевна- заведующая кафедрой специальных дисциплин Колледжа ДГУ, к.ю.н., доцент
Муртузалиева Аида Алиевна- старший преподаватель кафедры информационных технологий и безопасности компьютерных систем ДГУ

Рецензент:

Исмиханов З.Н. – к.э.н., доцент, зав. каф. информационных систем и технологий программирования факультета ИиИТ ДГУ

Рабочая программа дисциплины рассмотрена и рекомендована к утверждению на заседании кафедры специальных дисциплин Колледжа ДГУ.

Протокол № 8 от «30» 03 2022 г.

Зав. кафедрой _____ / Магомедова К.К./

Утверждена на заседании учебно-методического совета Колледжа ДГУ

Ст. методист _____ /Шамсутдинова У.А./

Рабочая программа дисциплины согласована с учебно-методическим управлением

«31» 03 2022 г. _____
подпись

2

Содержание

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Криптографические средства и методы защиты информации

1.1. Область применения программы

Рабочая программа дисциплины «Криптографические средства и методы защиты информации» является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 10.02.05. Обеспечение информационной безопасности автоматизированных систем для очного обучения студентов, имеющих основное общее образование, по программе базовой подготовки.

Рабочие программы дисциплин, адаптированные для обучения лиц с ограниченными возможностями здоровья, разрабатываются с учетом конкретных ограничений здоровья лиц, зачисленных в колледж, и утверждаются в установленном порядке.

1.2. Место дисциплины в структуре основной профессиональной образовательной программы:

Учебная дисциплина «Криптографические средства и методы защиты информации» относится к профессиональному модулю «Защита информации в автоматизированных системах программами и программно-аппаратными средствами» профессионального цикла ПССЗ.

1.3. Цели и задачи дисциплины – требования к результатам освоения дисциплины

«Криптографические средства и методы защиты информации»

Целью изучения дисциплины является получение обучающимися знаний в области защиты информационных систем с помощью криптографических методов защиты информации.

Задачами изучения дисциплины являются:

- изучение стандартов в области криптографической защиты информации;
- изучение основных методов шифрования;
- изучение базовых алгоритмов, применяемых в криптосистемах;
- освоение основ криптоанализа;
- изучение системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов.

Освоение содержания учебной дисциплины «Криптографические средства и методы защиты информации» обеспечивает достижение студентами следующих результатов:

Общие компетенции

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03.Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей уровня физической подготовленности.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.

Профессиональные компетенции

ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.

ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

В результате освоения дисциплины обучающийся должен **уметь:**

- использовать базовые знания теории чисел для реализации арифметических алгоритмов в криптографических системах;
  использовать частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки;
- уметь пользоваться научно- технической литературой в области криптографии;
- применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
- определять необходимость применения и выбирать сертифицированные 6 криптографические средства.

В результате освоения дисциплины обучающийся должен **знать:**

- арифметические алгоритмы, связанные с криптографическими системами
- основные задачи и понятия криптографии;
- требования к шифрам и основные характеристики шифров;
- модели шифров и математические методы их исследования;
- принципы построения криптографических алгоритмов;
- криптографические стандарты и их использование в информационных системах;
- перечень сертифицированных криптографических средств;
- угрозы безопасности;
- необходимость защиты информации в информационных системах;
- методы анализа безопасности компьютерных систем.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	*Объем часов*
Максимальная учебная нагрузка (всего)	***126***
Обязательная аудиторная учебная нагрузка (всего)	
в том числе:	
теоретическое обучение	*40*
лабораторные работы	
практические занятия (в т.ч. практическая подготовка)	*76*
контрольные работы	
курсовой проект	
консультация	
Самостоятельная работа обучающегося (всего)	*10*
в том числе:	
самостоятельная работа над курсовым проектом	
внеаудиторная самостоятельная работа	
Промежуточная аттестация в форме дифф. зачета	

2.2. Тематический план и содержание дисциплины «Криптографические средства и методы защиты информации»

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся, курсовая работ (проект) *(если предусмотрены)*	Объем часов
1	**2**	**3**
Раздел 1. Основные понятия и характеристика шифров		
Тема 1.1 Основные понятия. Криптографическая система. Классификация шифров.	**Содержание учебного материала**	**11**
	Криптография. Цели криптографии. История развития криптографии. Классификация криптографических методов. Обеспечение конфиденциальности, целостности, неотказуемости, аутентичности, неотслеживаемости информации. Основные понятия: шифр, открытый текст, шифр текст, электронная подпись, хэш-функция. Математические примитивы. Криптографические алгоритмы. Криптографическая схема. Криптографическая система. Классификация шифров.	*4*
	Практические занятия/ Лабораторные занятия	*6*
	1. Криптография. 2. Цели криптографии. 3. История развития криптографии. 4. Классификация криптографических методов. 5. Обеспечение конфиденциальности, целостности, неотказуемости, аутентичности, неотслеживаемости информации. 6. Основные понятия: шифр, открытый текст, шифр текст, электронная подпись, хэш-функция. 7. Математические примитивы. 8. Криптографические алгоритмы. 9. Криптографическая схема. 10. Криптографическая система. 11. Классификация шифров.	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос.	*1*
Тема 1.2 Алгебраическая модель шифра. Вероятностная модель шифра. Модели открытых текстов.	**Содержание учебного материала**	**11**
	Алгебраическая модель шифра. Алгебраическая модель шифра замены. Алгебраическая модель шифра перестановки. Алгебраическая модель шифра гаммирования. Вероятностная модель шифра. Распределения на множествах открытых текстов, ключей, шифр текстов. Математические модели открытых текстов.	*4*
	Практические занятия/ Лабораторные занятия	*6*

	1. Алгебраическая модель шифра. 2. Алгебраическая модель шифра замены. 3. Алгебраическая модель шифра перестановки. 4. Алгебраическая модель шифра гаммирования. 5. Вероятностная модель шифра. 6. Распределения на множествах открытых текстов, ключей, шифр текстов. 7. Математические модели открытых текстов.	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос.	*1*
Тема 1.3. Криптографическая и теоретическая стойкость шифров.	**Содержание учебного материала**	**11**
	Атаки на шифры. Понятие стойкости шифров. Классификация атак на шифры. Виды атак на схемы шифрования. Цели криптоанализа. Теоретико-информационная стойкость. Условная вероятность. Энтропия. Понятие абсолютно стойкого шифра. Теоретико-сложностная стойкость шифров. Понятие практической стойкости шифра. Модель противника.	*4*
	Практические занятия/ Лабораторные занятия	*6*
	1. Атаки на шифры. 2. Понятие стойкости шифров. 3. Классификация атак на шифры. 4. Виды атак на схемы шифрования. 5. Цели криптоанализа. 6. Теоретико-информационная стойкость. 7. Условная вероятность. 8. Энтропия. Понятие абсолютно стойкого шифра. 9. Теоретико-сложностная стойкость шифров. 10. Понятие практической стойкости шифра. 11. Модель противника.	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос. Подготовка доклада.	*1*
Раздел 2. Симметричная криптография		

Тема 2.1. Блочные и поточные шифры. Принципы построения блочных шифров	**Содержание учебного материала**	**11**
	Классификация симметричных криптографических систем. Требования к блочным шифрам. Требования к поточным шифрам. Криптографические параметры узлов и блоков блочных шифров. Базовые криптографические преобразования блочных шифров. Способы реализации блочных шифров. Процедура развертывания ключа	*4*
	Практические занятия/ Лабораторные занятия:	*6*
	1. Классификация симметричных криптографических систем. 2. Требования к блочным шифрам. 3. Требования к поточным шифрам. 4. Криптографические параметры узлов и блоков блочных шифров. 5. Базовые криптографические преобразования блочных шифров. 6. Способы реализации блочных шифров. 7. Процедура развертывания ключа	
	Консультации	
	Самостоятельная работа обучающихся: Тестирование, устный опрос	*1*
Тема 2.2. Сеть Фейстеля. Шифр DES. Поточные шифры.	**Содержание учебного материала**	**11**
	Сеть Фейстеля. Шифр DES. Основные преобразования. Алгоритм зашифрования. Алгоритм расшифрования. Процедура развертывания ключа. Типовые методы построения поточных шифров. Синхронные и самосинхронизирующиеся поточные шифры. Генераторы псевдослучайных последовательностей. Статистические характеристики генераторов псевдослучайных последовательностей. Методы усложнения последовательностей.	*4*
	Практические занятия/ Лабораторные занятия:	*6*
	1. Сеть Фейстеля. 2. Шифр DES. 3. Основные преобразования. 4. Алгоритм зашифрования. 5. Алгоритм расшифрования. Процедура развертывания ключа. 6. Типовые методы построения поточных шифров. 7. Синхронные и самосинхронизирующиеся поточные шифры. 8. Генераторы псевдослучайных последовательностей. 9. Статистические характеристики генераторов псевдослучайных последовательностей. Методы усложнения последовательностей.	

	Консультации	
	Самостоятельная работа обучающихся: Доклад, разработка презентации к докладу на семинаре, поиск информации в сетях.	*1*
Раздел 3. Криптография с открытым ключом		
Тема 3.1. Односторонние функции, функции с секретом	**Содержание учебного материала**	**11**
	Элементы теории сложности. Односторонние функции. Односторонние функции с секретом. Примеры односторонних функций с секретом. Алгебраическая модель асимметричного шифра. Понятие открытого ключа.	*4*
	Практические занятия/ Лабораторные занятия:	*6*
	1. Элементы теории сложности. 2. Односторонние функции. 3. Односторонние функции с секретом. 4. Примеры односторонних функций с секретом. 5. Алгебраическая модель асимметричного шифра. 6. Понятие открытого ключа.	
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить сообщение по теме: Коммуникационное оборудование. Технология локальных сетей.	*1*
Тема 3.2. Схемы шифрования RSA и Эль-Гамаля	**Содержание учебного материала**	**11**
	Схема шифрования RSA. Процедура генерации ключей. Процедура шифрования. Схема Эль-Гамаля. Стойкость схем шифрования RSA и Эль-Гамаля.	*4*
	Практические занятия/ Лабораторные занятия:	*6*
	1. Схема шифрования RSA. 2. Процедура генерации ключей. 3. Процедура шифрования. 4. Схема Эль-Гамаля. 5. Стойкость схем шифрования RSA и Эль-Гамаля.	
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить сообщение по теме: Коммуникационное оборудование. Технология локальных сетей.	*1*
Раздел 4. Электронная подпись.		

Тема 4.1. Понятие электронной подписи. Способы построения электронной подписи	**Содержание учебного материала**	**11**
	Понятие электронной подписи. Связь с понятием электронной подписи ФЗ-63. Процессы формирования и проверки электронной подписи. Алгебраическая модель схемы электронной подписи. Конструкция схемы электронной подписи на односторонней функции с секретом. Электронная подпись на основе схемы шифрования с открытым ключом, электронная подпись с извлечением сообщения, электронная подпись с дополнением.	*4*
	Практические занятия/ Лабораторные занятия:	*6*
	1. Понятие электронной подписи. 2. Связь с понятием электронной подписи ФЗ-63. 3. Процессы формирования и проверки электронной подписи. 4. Алгебраическая модель схемы электронной подписи. 5. Конструкция схемы электронной подписи на односторонней функции с секретом. 6. Электронная подпись на основе схемы шифрования с открытым ключом, электронная подпись с извлечением сообщения, электронная подпись с дополнением.	
	Консультации	
	Самостоятельная внеаудиторная работа: Подготовить доклад по теме.	*1*
Тема 4.2. Криптографическая хэш-функция	**Содержание учебного материала**	**11**
	Криптографическая хэш-функция без ключа. Слабая хэш-функция. Сильная хэшфункция. Стойкость криптографической хэш-функции. Применение хэш-функций. Типовые конструкции криптографических хэш-функций. Хэш-функция ГОСТ Р 34.11–94. Конструкция хэш-функции на основе алгоритма шифрования. Шаговая функция хэширования.	*2*
	Практические занятия/ Лабораторные занятия:	*8*
	1. Криптографическая хэш-функция без ключа. 2. Слабая хэш-функция. Сильная хэшфункция. 3. Стойкость криптографической хэш-функции. 4. Применение хэш-функций. 5. Типовые конструкции криптографических хэш-функций. 6. Хэш-функция ГОСТ Р 34.11–94. 7. Конструкция хэш-функции на основе алгоритма шифрования. 8. Шаговая функция хэширования.	
	Самостоятельная внеаудиторная работа: Подготовить доклад по теме.	*1*

Раздел 5. Применение криптографических методов и средств для обеспечения информационной безопасности		
Тема 5.1. Коды аутентификации сообщений. Криптографические протоколы	**Содержание учебного материала**	**11**
	Коды аутентификации сообщений. Методы построения кодов аутентификации сообщений. Основные понятия. Цели безопасности криптографических протоколов. Протоколы передачи сообщений. Протоколы передачи ключей. Протоколы аутентификации.	*2*
	Практические занятия/ Лабораторные занятия:	*8*
	1. Коды аутентификации сообщений. 2. Методы построения кодов аутентификации сообщений. 3. Основные понятия. Цели безопасности криптографических протоколов. Протоколы передачи сообщений. 4. Протоколы передачи ключей. **5.** Протоколы аутентификации.	
	Консультации	
	Самостоятельная внеаудиторная работа: Работа с учебной литературой, выполнение домашнего задания.	*1*
Тема 5.2. Управление ключами. Инфраструктура открытых ключей	**Содержание учебного материала**	**10**
	Универсальная модель жизненного цикла ключа. Управление ключами. Службы управления ключами. Назначение инфраструктуры открытых ключей. Удостоверяющий центр. Функции удостоверяющего центра. Сертификат открытого ключа	*2*
	Практические занятия/ Лабораторные занятия:	*8*
	1. Универсальная модель жизненного цикла ключа. 2. Управление ключами. 3. Службы управления ключами. 4. Назначение инфраструктуры открытых ключей. 5. Удостоверяющий центр. 6. Функции удостоверяющего центра. 7. Сертификат открытого ключа	
	Консультации	
	Самостоятельная внеаудиторная работа	
Тема 5.3. Принципы разработки и модернизации СКЗИ. Нормативное обеспечение КМЗИ	**Содержание учебного материала**	**7**
	Общие принципы построения СКЗИ. Принципы применения криптографических механизмов защиты. Принципы применения инженерно-криптографических механизмов защиты. Положение ПКЗ-2005.Положение о лицензировании деятельности по разработке, производству,	*2*

	распространению шифровальных (криптографических) средств. Приказ ФАПСИ 152. Приказ ФСБ РФ 378.	
	Практические занятия/ Лабораторные занятия:	*4*
	1. Общие принципы построения СКЗИ. 2. Принципы применения криптографических механизмов защиты. 3. Принципы применения инженерно-криптографических механизмов защиты. Положение ПКЗ-2005. **4.** Положение о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств. Приказ ФАПСИ 152. Приказ ФСБ РФ 378.	
	Самостоятельная внеаудиторная работа	
Примерная тематика курсовой работы (проекта) *(если предусмотрены)*		*не предусмотрено*
Самостоятельная работа обучающихся над курсовой работой (проектом) *(если предусмотрены)*		*не предусмотрено*
Всего:		***126***

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Учебная аудитория для проведения лекционных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Оснащение аудитории:

- комплект учебной мебели: парты, стол преподавательский, стулья, доска;
- мультимедийная система: проектор, экран настенный, ноутбук.

Программное обеспечение ноутбука лекционных аудиторий:

- лицензионное программное обеспечение:
- ОС Microsoft Windows;
- свободно распространяемое программное обеспечение:
- офисный пакет LibreOffice;
- программа просмотра pdf-документов Sumatra PDF Reader.

Практические занятия проводятся в кабинете интернет-технологий и информатики, оборудованным ПЭВМ с установленным программным обеспечением:

- лицензионное программное обеспечение:
- ОС Microsoft Windows;
- свободно распространяемое программное обеспечение:
- офисный пакет LibreOffice;
- система программирования «Microsoft Visual Studio Express»;
- программа просмотра pdf-документов Sumatra PDF Reader.

Для самостоятельной работы студентов используется кабинет интернет-технологий и информатики.

Оснащение кабинета:

- комплект учебной мебели: стол преподавательский, столы компьютерные, стулья
- персональные компьютеры, сетевой коммутатор, сетевая кабельная система.

Программное обеспечение:

- лицензионное программное обеспечение:
- ОС Microsoft Windows
- Антивирус Касперского
- свободно распространяемое программное обеспечение:
- офисный пакет LibreOffice;
- программа просмотра pdf-документов Sumatra PDF Reader.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основная литература:

1. Запечников, С. В. Криптографические методы защиты информации : учебник для сузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2022. — 309 с. — (профессиональное образование). — ISBN 978-5-534-02574-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489487

2. Запечников, С. В. Криптографические методы защиты информации : учебник для сузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. - Москва : Издательство Юрайт, 2021. - 309 с. - (Профессиональное образование). - ISBN 978-5-534-02574-3. - Текст :

электронный // Образовательная платформа Юрайт [сайт]. - URL: https://urait.ru/bcode/468902

3. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для сузов / И. Н. Васильева. - Москва : Издательство Юрайт, 2020. - 349 с. - (Профессиональное образование). - ISBN 978-5-534-02883-6. - Текст : электронный // Образовательная платформа Юрайт [сайт]. - URL: https://urait.ru/bcode/450998

4. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — URL : https://urait.ru/bcode/476997

Дополнительная литература:

1. Коржик В.И. Основы криптографии [Электронный ресурс]: Учебное пособие/ Коржик В.И., Яковлев В.А.- Электронно - текстовые данные.- СПб.:Интермедия, 2017.- 312 с.- Режим доступа: http://www.bibliocomplectator.ru/book/?id=66798.-
2. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2021. — 424 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — URL : https://urait.ru/bcode/469133
3. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2022. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — URL : https://urait.ru/bcode/489745
4. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2021. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — URL : https://urait.ru/bcode/470279

Интернет-ресурсы:

1. Библиотека Альдебаран – компьютерная литература [Электронный ресурс]. – Режим доступа: http://www.aldebarans.ru/komp, свободный. – Загл. с экрана.
2. Википедия – Свободная энциклопедия [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org, свободный. – Загл. с экрана.
3. Официальный сайт Министерства образования и науки Российской Федерации. – Режим доступа: http://www.mon.gov.ru, свободный. – Загл. с экрана.
4. Педагогика.ру – Справочный сайт [Электронный ресурс]. – Режим доступа: http://www.pedagogy.ru, свободный. – Загл. с экрана.
5. Портал нормативно-технической документации [Электронный ресурс]. – Режим доступа: http://www.pntdoc.ru, свободный. – Загл. с экрана.
6. Российское образование. Федеральный портал [Электронный ресурс].. – Режим доступа: http://www.edu.ru, свободный. – Загл. с экрана.
7. Техническая литература [Электронный ресурс]. – Режим доступа: http://www.tehlit.ru, свободный. – Загл. с экрана

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
В результате освоения дисциплины обучающийся должен **уметь:** - применять математические методы описания и исследования криптографических систем; - осуществлять рациональный выбор криптографических методов и средств защиты информации в телекоммуникационных системах; - реализовывать типовые криптографические преобразования; - безопасно настроить сетевое устройство и программное обеспечении инфокоммуникационной системы; - проводить анализ безопасности компьютерных систем на соответствие стандартам безопасности; - выполнять программную реализацию алгоритмов криптозащиты для шифрования данных; - использовать на практике криптографические методы защиты информации.	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной работы; тестирование; рефераты; составление и оформление письменных документов; подготовка и защита рефератов; Экспертная оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач.
В результате освоения дисциплины обучающийся должен **знать:** - модели шифров и математические методы их исследования - основные задачи и понятия криптографических методов защиты информации; - основные криптографические методы защиты информации; - требования к шифрам и основные характеристики шифров - правовые основы защиты информации в компьютерных системах; - атаки и угрозы безопасности; - каналы утечки информации; - закон об охране программ для ЭВМ и баз данных; - закон о защите личных данных правовые основы защиты информации в компьютерных системах; - основы информационной защиты; - принципы управления сетевыми устройствами; - основы настройки программного обеспечения инфокоммуникационной системы.	Интерпретация результатов устного опроса. Текущий контроль в форме тестирования. Текущий контроль усвоения материала в форме комбинированного опроса. Экспертная оценка результатов выполнения домашнего задания. Текущий контроль в форме комбинированного опроса. Экспертная оценка результатов выполнения домашнего задания.