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

Колледж

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

МДК 05.02 Криптографические методы защиты информации

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

Специальность:	*09.02.07 Информационные системы и программирование*
Обучение:	*по программе базовой подготовки*
Уровень образования, на базе которого осваивается ППССЗ:	*основное общее образование*
Квалификация:	*программист*
Форма обучения:	*очная*

Махачкала - 2020

Рабочая программа дисциплины «Криптографические методы защиты информации» составлена в 2021 году в соответствии с требованиями ФГОС СОО от 17 мая 2012г. №413, ФГОС СПО от 9 декабря 2016 г. N 1547 по специальности 09.02.07 Информационные системы и программирование для реализации основной профессиональной образовательной программы СПО на базе основного общего образования с получением среднего общего образования.

Организация-разработчик: колледж федерального государственного бюджетного образовательного учреждение высшего образования «Дагестанский государственный университет» (Колледж ДГУ)

Разработчики:

Ахмедова Н.М. – старший преподаватель кафедры ИСиТП факультета ИиИТ

Рабочая программа дисциплины одобрена на заседании кафедры специальных дисциплин Колледжа ДГУ
протокол №_8_ от «26» _марта_ 2020г.

Зав. кафедрой _____/Магомедова А.М./

Рабочая программа дисциплины согласована с учебно-методическим управлением «26» _03_ 2020г.

Начальник УМУ, д.б.н., проф. _____ Гасангаджиева А.Г.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Криптографические методы защиты информации

1.1. Область применения программы

Рабочая программа дисциплины является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 09.02.07 Информационные системы и программирование *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 методы защиты информации» относится к профессиональному модулю «Разработка децентрализованных приложений» профессионального цикла ПССЗ.

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

Целью освоения дисциплины является изучение основных математических подходов к решению задач компьютерной безопасности и, прежде всего, к построению актуальных криптографических алгоритмов с учетом применения современных цифровых технологий.

Задачи дисциплины:

- Формирование знаний системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов;
- Формирование умений принципов синтеза и анализа шифров;
- Приобретение навыков математических методов, используемых в криптоанализе.

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 10. Пользоваться профессиональной документацией на государственном и иностранном языке.

Профессиональные компетенции

ПК 11.6. Защищать информацию в базе данных с использованием технологии защиты информации.

В результате освоения дисциплины обучающийся должен уметь:

- применять математические модели для оценки стойкости СКЗИ
- использовать в автоматизированных системах
- пользоваться нормативными документами в области технической защиты информации

В результате освоения дисциплины обучающийся должен знать:

- основные понятия и задачи криптографии
- основные алгоритмы хеширования
- математические модели криптографических систем
- способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации

При реализации содержания учебной дисциплины «Криптографические методы защиты информации» в пределах освоения ОПОП СПО на базе основного общего образования с получением среднего общего образования учебная нагрузка студентов составляет 112 часов, из них аудиторная (обязательная) учебная нагрузка, включая практические занятия, — 92 часов; внеаудиторная самостоятельная работа студентов — 20 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	***Объем часов***
Максимальная учебная нагрузка (всего)	*112*
Обязательная аудиторная учебная нагрузка (всего)	*92*
в том числе:	
теоретическое обучение	*32*
лабораторные работы	
практические занятия	*60*
контрольные работы	
курсовой проект	
Самостоятельная работа обучающегося (всего)	*20*
в том числе:	
самостоятельная работа над курсовым проектом	
внеаудиторная самостоятельная работа	*20*
Промежуточная аттестация в форме дифф.зачета	

2.2. Тематический план и содержание дисциплины Криптографические методы защиты информации

наименование дисциплины

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.	*Введение в криптографию.*	
Тема 1.1 Введение криптографию	Содержание учебного материала	*6*
	1 Основные понятия криптографии. Введение в криптографию.	
	2 Криптографические атаки. Криптографический протокол.	
	Практические занятия/ Лабораторные занятия	*10*
	1 Шифрование с закрытым ключом незнакомого теста.	
	2 Одноалфавитная замена. Пропорциональные шифры.	
	Консультации	
	Самостоятельная работа обучающихся	*4*
Тема 1.2 Краткая история криптографии	Содержание учебного материала	*6*
	1 Краткая история криптографии	
	2 Исторические шифры**.** Устройство. Эволюция шифров.	
	Практические занятия/ Лабораторные занятия	*10*
	Многоалфавитные подстановки, методы гаммирования. Методы перестановки. Понятие композиционного шифра	
	Консультации	
	Самостоятельная работа обучающихся	*4*
Раздел 2.	Симметричное и ассиметричное шифрование	
Тема 2.1. Шифр Цезаря.	Содержание учебного материала	*6*
	1 Простейшие методы шифрования с закрытым ключом.	
	2 Шифр простой замены.	
	Практические занятия/ Лабораторные занятия	*10*
	Программная реализация шифра Цезаря.	
	Консультации	

	Самостоятельная работа обучающихся	*4*
Тема 2.2. Шифр Виженера.	Содержание учебного материала	*6*
	1. Таблица Виженера.	
	2. Частотный анализ.	
	Практические занятия/ Лабораторные занятия	*10*
	Программная реализация шифра Вижинера.	
	Консультации	
	Самостоятельная работа обучающихся	*4*
Раздел 3.	Алгоритмы хеширования	
Тема 3.1 Блочное шифрование. Сеть Фейстеля.	Содержание учебного материала	*4*
	1. Принципы построения блочных шифров с закрытым ключом	
	2. Режимы работы блочных шифров. Сеть Фейштеля.	
	Практические занятия/ Лабораторные занятия	*10*
	Использование алгоритма хеширования для сокрытия содержимого файла. Использование алгоритма хеширования для подтверждения неизменности файла	
	Консультации	
	Самостоятельная работа обучающихся	*2*
Тема 3.2 DES/3DES	Содержание учебного материала	*4*
	1. Алгоритмы шифрования DES и 3DES. Общие сведения. Шифрование и расшифрование	
	2. Алгоритмы шифрования AES. Общие сведения.	
	Практические занятия/ Лабораторные занятия	*10*
	Поточные шифры. DES-шифрование.	
	Консультации	
	Самостоятельная работа обучающихся	*2*
Примерная тематика курсовой работы (проекта) *(если предусмотрены)*		
Самостоятельная работа обучающихся над курсовой работой (проектом) *(если предусмотрены)*		
	Всего:	*112*

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия учебного кабинета. Для усвоения знаний и практических навыков студентами изучение дисциплины обеспечено, прежде всего, наличием учебного кабинета, в котором есть возможность проводить занятия, как в традиционной форме, так и с использованием интерактивных технологий и различных образовательных методик.

Оборудование учебного кабинета: - посадочные места по количеству обучающихся; - рабочее место преподавателя; - комплект учебно-наглядных пособий;

Технические средства обучения: - проектор; - интерактивная доска.

3.2. Информационное обеспечение обучения
Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основная литература:

1. 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/469758
2. Торстейнсон П. Криптография и безопасность в технологии .NET / Торстейнсон П., Ганеш Г.А.. — Москва : Лаборатория знаний, 2020. — 480 c. — ISBN 978-5-00101-700-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/20709.html — Режим доступа: для авторизир. пользователей
3. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для сузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2020. — 209 с. — (Профессиональное образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/469567
4. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для сузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2020. — 245 с. — (Профессиональное образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/470279

Дополнительная литература:

1. Иванов, Михаил Александрович. Методы и средства криптографической защиты информации в компьютерных системах и сетях. - М. : КУДРИЦ-ОБРАЗ, 2001. - 363 с. - ISBN 5-93378- 021-9 : 0-0..

2. Калмыков И.А. Методы и средства криптографической 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
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
4. Лоран Л. Блокчейн от А до Я; Все о технологии десятилетия. М: Бомбора, 2017. – 376с. – ISBN 978-5-699-98942-3
5. Практикум по выполнению лабораторных работ по дисциплине Методы и средства криптографической 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
6. Табернакулов А., Койфманн Я. Блокчейн на практике. М.: Альпина Паблишер, 2019, 260 с. - ISBN 978-5-9614-2382-2
7. 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
8. Учебно-методическое пособие по выполнению курсовой работы по дисциплине Методы и средства криптографической 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

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

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

1) 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/ .

2) 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.

3) Информационный портал по безопасности **SecurityLab.ru**, новости, статьи, обзор уязвимостей, вирусов и мнения аналитиков.

4) Алгоритмы хеширования криптовалют в 2020 году – Режим доступа: https://www.developcoins.com/cryptocurrency-hashing-algorithms
5) Secure Hash Algorithms – Режим доступа: https://brilliant.org/wiki/secure-hashing-algorithms/.

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**
Знать: – основные понятия и задачи криптографии – основные алгоритмы хеширования – математические модели криптографических систем – способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации Уметь: – применять математические модели для оценки стойкости СКЗИ – использовать в автоматизированных системах – пользоваться нормативными документами в области технической защиты информации	Самостоятельная работа по темам; Наблюдение за выполнением практического задания. (деятельностью студента); Оценка выполнения практического задания(работы); Решение ситуационной задачи при выполнении практических заданий; Контрольная работа