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

Колледж

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.05 РАЗРАБОТКА ДЕЦЕНТРАЛИЗОВАННЫХ ПРИЛОЖЕНИЙ

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 «ПМ.05 Разработка децентрализованных приложений» разработана на основе требований Федерального государственного образовательного стандарта (ФГОС) среднего профессионального образования (СПО) по специальности 09.02.07. Информационные системы и программирование от 09.12.2016 №1547 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:

Магомедова А.М. – преподаватель кафедры специальных дисциплин Колледжа ДГУ
Магомедгаджиев Ш.М., к.э.н., доцент, доцент кафедры «Информационных систем и технологий программирования»
Ахмедова Н.М. – старший преподаватель кафедры ИСиТП факультета ИиИТ
Зубаирова Р.У. – преподаватель кафедры специальных дисциплин Колледжа ДГУ

Рабочая программа профессионального модуля рассмотрена и рекомендована к утверждению на заседании кафедры специальных дисциплин колледжа ДГУ

Протокол № 7 от «27» 02 2021г.

Зав. кафедрой _____ /Магомедова А.М./

Рабочая программа профессионального модуля согласована с учебно-методическим управлением
«16» 03 2021 г. _____
(подпись)

Программа профессионального модуля согласована с представителем работодателя
Нач. отдела развития цифровых технологий и координации информатизации Минцифры
(полное наименование организации и должности руководителя)
Ильясов Мурад Алиевич _____ (подпись)
ФИО

2

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.05 РАЗРАБОТКА ДЕЦЕНТРАЛИЗОВАННЫХ ПРИЛОЖЕНИЙ

1.1. Область применения программы

Рабочая программа профессионального модуля ПМ.05 Разработка децентрализованных приложений 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:

Профессиональный модуль «ПМ.05 Разработка децентрализованных приложений» относится к профессиональному циклу ПССЗ.

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

С целью овладения указанным видом профессиональной деятельности, обучающийся в ходе освоения профессионального модуля должен:

уметь:

- правильно выбирать и применять технологию
- правильно выбирать и применять шаблоны и алгоритмы при разработке
- использовать технологии блокчейн;
- применять криптографические основы технологии блокчейн;
- создавать блокчейн-приложения на открытых платформах.
- применять математические модели для оценки стойкости СКЗИ
- использовать в автоматизированных системах
- пользоваться нормативными документами в области технической защиты информации

знать:

- основы технологии, сферы и назначение блокчейн-технологии;
- принципы работы блокчейн-технологии;
- формирование транзакций;
- формирование блоков, механизмы консенсусов, передача блоков.
- криптографические основы технологии блокчейн;
- технологии создания блокчейн-приложений на открытых платформах.
- 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

Освоение содержания учебной дисциплины 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 10. Пользоваться профессиональной документацией на государственном и иностранном языке.

Профессиональные компетенции

ПК-11.1. Осуществлять сбор, обработку и анализ информации для проектирования баз данных.

ПК-11.2. Проектировать базу данных на основе анализа предметной области.

ПК-11.3. Разрабатывать объекты базы данных в соответствии с результатами анализа предметной области.

ПК-11.4. Реализовывать базу данных в конкретной системе управления базами данных.

ПК-11.5. Администрировать базы данных.

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

1.3. Количество часов на освоение программы профессионального модуля:

всего – 297 часов, в том числе:

- максимальной учебной нагрузки обучающегося – 225 часов,

включая:

- обязательной аудиторной учебной нагрузки обучающегося – 184 часа;
- самостоятельной работы обучающегося – 40 часов;
- консультации – 1 часа;
- производственной практики – 72 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Код общих и профессиональных компетенций	Наименование разделов профессионального модуля	Всего, часов	Объем профессионального модуля, час.					
			Работа обучающихся во взаимодействии с преподавателем					Самостоятельная работа
			Обучение по МДК			Практики		
			Всего	В том числе		учебная	производственная	всего
				лабораторные и практические занятия	курсовая работа (проект)			
1	2	3	4	5	6	7	8	9
ПК 1-4; ПК-10; ПК 11.1-11.5	**МДК.05.01 Технология Blockchain**	**113**	**93**	60				20
ПК 1-4; ПК-10; ПК 11.6	**МДК.05.02 Криптографические методы защиты информации**	**112**	**92**	60				20
ПК 1-4; ПК-10; ПК 11.1-11.6	**Производственная практика, (по профилю специальности),** часов	**72**						
	Всего:	**297**	**183**	**120**	**-**		**72**	**40**

2.2. Тематический план и содержание дисциплины «ПМ.05 Разработка децентрализованных приложений»

2.2. Тематический план и содержание профессионального модуля

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся, курсовая работ (проект) *(если предусмотрены)*	Объем часов
1	**2**	**3**
МДК.05.01 Технология Blockchain		**113**
Раздел 1.	**Принципы работы технологии блокчейн**	*56*
Тема 1.1 Введение в блокчейн-технологии	Содержание учебного материала	*8*
	Основные идеи, лежащие в основе блокчейн-технологий: децентрализация, распределенный реестр, цепочка блоков, достижение консенсуса. Техническая реализация систем распределенного реестра: транспортный уровень, уровень хранения данных, прикладной уровень. Одноранговые (пиринтовые) сети как основа транспортного уровня. Понятие ноды. Взаимодействие клиентов с нодами. Сетевая структура БД (ациклический ориентированный граф) как основа уровня хранения данных. Смарт-контракты как основа прикладного уровня. Простейшие примеры смарт-контрактов.	
	Практические занятия 1. Знакомство с существующими блокчейн-технологиями. 2. Введение в порядок разворачивания блокчейн-инфраструктуры.	*14*
	Консультации	-
	Самостоятельная работа обучающихся Краткий очерк истории развития блокчейн-технологий. Открытые (permissionless) и частные (permissioned) блокчейн-платформы, их сравнение. Отличия открытых и частных блокчейн-платформ. Основные проблемы блокчейн-платформ: безопасность и масштабируемость	*6*
Тема 1.2 Основы криптографии	Содержание учебного материала	*8*
	Криптография как наука о безопасности связи. Основные понятия криптографии. Симметричная и асимметричная криптография. Основы симметричной криптографии. Шифры замены и шифры перестановки, их композиции. Классические шифры. Шифр Вернама. Совершенная секретность по Шеннону. Одноразовый шифрблокнот. Симметричное шифрование. Современные практически стойкие шифры. Блочные и поточные шифры. Понятия однонаправленной функции, однонаправленной функции с секретом (с потайной дверью). Основные алгебраические структуры, используемые в криптографии: группы, кольца, поля. Примеры алгебраических структур, используемых в криптографии. Открытое распределение ключей. Электронная цифровая подпись (ЭЦП). Применение ЭЦП для контроля подлинности. Совместное применение ЭЦП и хэш-функции. Схема подписи RSA. Криптографическая хэш-функция. Свойства хэш-	

	функции: сжатие, однонаправленность, трудность обнаружения коллизий. Применение хэш-функции для контроля целостности данных. Функции криптографии в блокчейн-платформах.	
	Практические занятия 1. Основы криптографии. Хеширование. 2. Криптография с открытым ключом. 3. Инфраструктура криптографии с открытым ключом. 4. Применение криптографии с открытым ключом в информационной безопасности. 5. Применение криптографии с открытым ключом в блокчейн-технологиях. 6. Доказательство с нулевым разглашением. Определение децентрализованных приложений.	*16*
	Консультации	-
	Самостоятельная работа обучающихся ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Российский стандарт подписи ГОСТ Р 34.10-2012. Российский стандарт хэш-функции ГОСТ Р 34.11-2012.	*4*
Раздел 2.	**Практическое применение блокчейн технологий**	*57*
Тема 2.1. Принципы функционирования блокчейн-платформ	Содержание учебного материала	*8*
	Хранение данных в системах распределенного реестра. Формирование блоков транзакций. Дерево Меркле. Формирование цепочки блоков. Достижение консенсуса в блокчейн-платформах открытого типа путем доказательства выполнения работы (proof-of-work), используемая при этом вычислительно сложная задача подбора значения хэш-функции. Вознаграждение нод, майнинг криптовалют. Особенности доказательства выполнения работы: регулирование сложности задачи, разрешение вилок (forks). Атака 51%. Способы достижения консенсуса в блокчейн-платформах закрытого типа.	
	1. Практические занятия 2. Обзоры основных платформ для создания блокчейн-проектов, их отличия друг от друга. 3. Блоки, механизмы сцепления блоков и целостность цепочки. 4. Основные сведения блокчейна Bitcoin. 5. Адреса и транзакции. Структура блока. 6. Требования сложности и схемы работы майнингового алгоритма. 7. Основные сведения и отличия блокчейна Etherium. 8. Введение в консенсус и его определение. Консенсус Proof Of Work. 9. Задача византийских генералов и другие виды консенсуса. 10. Ветвление. Генезис. 11. Виртуальная машина Etherium. Создание аккаунта. Изучение средств для мониторинга блокчейн-сети.	*14*
	Консультации	*1*
	Самостоятельная работа обучающихся Фундаментальные теоремы о консенсусе. «Задача о византийских генералах» и её решения для случаев	*6*

	подписанных и неподписанных сообщений. Протоколы византийского соглашения, их характерные особенности и пороги устойчивости к воздействию злоумышленника	
Тема 2.2. Сферы применения блокчейн-технологий	Содержание учебного материала	*8*
	Чисто реестровые приложения блокчейн-технологий: криптовалюты, доказательная регистрация событий и пр. Блокчейн как платформа децентрализованных вычислений. Смарт-контракты. Примеры смарт-контрактов. Языки программирования смарт-контрактов. Приложения, основанные на использовании блокчейна как платформы децентрализованных вычислений: управление цепочками поставок, отслеживание происхождения товаров, электронные договоры и сделки, медицинские информационные системы. Краудсорсинговые применения	
	1. Практические занятия 2. Базовые понятия смарт-контракта. Структура смарт-контракта. 3. Расположение данных. Управляющие структуры. Свойства контракта. 4. Доказательство наличия, целостности и принадлежности файла. 5. Создание контракта. Языки программирования смарт-контрактов. 6. Компиляция и развертывание смарт-контракта. 7. Платформа для смарт-контрактов. Введение в разработку смарт-контрактов уровня предприятия.	*16*
	Консультации	
	Самостоятельная работа обучающихся Изучение языка программирования Solidity и практика создания смарт-контрактов на данном языке. Знакомство с web3.js.	*4*
МДК 05.02 Криптографические методы защиты информации		***112***
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	Содержание учебного материала	*6*
	1 Краткая история криптографии	

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*
Производственная практика		***72 ч***
Итого		***297ч***

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы профессионального модуля требует наличия учебного кабинета / учебной лаборатории «Программирования и баз данных».

Оборудование кабинета и рабочих мест кабинета «Информатики и информационных технологий в профессиональной деятельности»:

- автоматизированные рабочие места на 12-15 обучающихся (Процессор не ниже Core i3, оперативная память объемом не менее 8 Гб);
- автоматизированное рабочее место преподавателя (Процессор не ниже Core i3, оперативная память объемом не менее 8 Гб);
- проектор и экран;
- маркерная доска;

Программное обеспечение общего и профессионального назначения, в том числе включающее в себя следующее ПО:

MS'SQL Server MS'SQL Server Management Studio MS'Visual Studio 2008 Open Office Office 2010 Professional Windows 7 Professional 7-Zip AcrobatReader.

Технические средства обучения: сервер в лаборатории (8-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 16 Гб, жесткие диски общим объемом не менее 1 Тб, программное обеспечение: WindowsServer 2012 или более новая) или выделение аналогичного по характеристикам виртуального сервера из общей фермы серверов.

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 с. — 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.

1. eLIBRARY.RU [Электронный ресурс]: электронная библиотека / Науч.

электрон. б-ка. – Москва, 1999 –. Режим доступа: http://elibrary.ru/defaultx.asp. – 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
3. любой точки, имеющей доступ в интернет. – URL: http://moodle.dgu.ru/ .

4. 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.
5. Информационный портал по безопасности **SecurityLab.ru**, новости, статьи, обзор уязвимостей, вирусов и мнения аналитиков.
6. Алгоритмы хеширования криптовалют в 2020 году – Режим доступа: https://www.developcoins.com/cryptocurrency-hashing-algorithms
7. 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 и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Перечень умений, осваиваемых в рамках дисциплины: У1 правильно выбирать и применять технологию У2 правильно выбирать и применять шаблоны и алгоритмы при разработке использовать технологии блокчейн; У3 применять криптографические основы технологии блокчейн; У4 создавать блокчейн-приложения на открытых платформах. Перечень знаний, осваиваемых в рамках дисциплины: З1 основы технологии, сферы и назначение блокчейн-технологии;	Самостоятельная работа по темам; Тестирование по разделам и темам; Наблюдение за выполнением практического задания. (деятельностью студента); Оценка выполнения практического задания(работы); Решение ситуационной задачи при выполнении практических заданий;

32 принципы работы блокчейн-технологии; формирование транзакций; 33 формирование блоков, механизмы консенсусов, передача блоков; 34 криптографические основы технологии блокчейн; 35 технологии создания блокчейн-приложений на открытых платформах.	
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