МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет компьютерных технологий и прикладной математики



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ Б1.О.26 «КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ»

Направление подготовки/специальность_02.03.02 **Фундаментальная информатика и информационные технологии**
(код и наименование направления подготовки/специальности)

Направленность (профиль) / специализация
Математическое и программное обеспечение компьютерных технологий
(наименование направленности (профиля) специализации)

Программа подготовки _академический бакалавриат
(академическая /прикладная)

Форма обучения____очная
(очная, очно-заочная, заочная)

Квалификация (степень) выпускника_____бакалавр
(бакалавр, магистр, специалист)

Краснодар 2019

Рабочая программа дисциплины «Криптографические протоколы» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 02.03.02 Фундаментальная информатика и информационные технологии

Программу составил: А.С. Жук старший преподаватель
кафедры вычислительных технологий

Рабочая программа дисциплины утверждена на заседании кафедры вычислительных технологий от «26 » апреля 2019 г., протокол № 7

Заведующий кафедрой (разработчика) Вишняков Ю.М.



Рабочая программа дисциплины утверждена на заседании кафедры вычислительных технологий от «26 » апреля 2019 г., протокол № 7

Заведующий кафедрой (выпускающей) Вишняков Ю.М.



Утверждена на заседании учебно-методической комиссии факультета компьютерных технологий и прикладной математики протокол № 1 от «15» мая 2019 г.

Председатель УМК факультета Коваленко А.В.



Рецензенты:

Схаляхо Ч.А. , доцент КВВУ им.С.М.Штеменко, к.ф.-м.н., доцент

Гаркуша О.В., доцент кафедры информационных технологий ФБГОУ ВО «Кубанский государственный университет», кандидат физико-математических наук, доцент.

1. Цели и задачи изучения дисциплины (модуля)

1.1 Цель освоения дисциплины

Целью преподавания и изучения дисциплины «Дискретная математика» является формирование у студентов знаний и навыков по использованию методов согласованного решения задач информационного обмена с использованием криптографии.

1.2 Задачи дисциплины

Студент должен **знать** о основные алгоритмы, методы и средства криптографии; **уметь** применять теории, методы, алгоритмы криптографии; **владеть** знаниями теории, методов, алгоритмов построения криптографических протоколов для решения теоретических проблем фундаментальной информатики и практических задач информационных технологий.

1.3 Место дисциплины (модуля) в образовательной программе

Дисциплина «Криптографические протоколы» относится к профессиональной части обязательных дисциплин.

Для изучения дисциплины необходимо знания, полученные при изучении дисциплин дискретная математика, алгебра, методы программирования, основы теории вероятностей и статистических методов, компьютерные сети, конструирование алгоритмов и структур данных, программирование в компьютерных сетях, информационная безопасность. Знания, получаемые при изучении дисциплины Криптографические протоколы, используются при изучении магистерских дисциплин и служат основой для написания научно-исследовательской работы и выпускной квалификационной работы..

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотне- сенных с планируемыми результатами освоения образовательной программы

Изучения данной учебной дисциплины направлено на формирование у обучающихся следующих **общепрофессиональных компетенций**:

№ п.п	Индекс компе-тенции	Содержание компетенции (или ее части)	В результате изучения учебной дисциплины обучающиеся должны		
			Знать	Умет ь	Владеть
1	ОПК-5	Способен инсталлировать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности	Основные принципы работы криптографически х протоколов	инсталлировать и сопровождать программное обеспечение информационных систем с применением криптографическ их протоколов	Способностью оценивать эффективность работы криптографичес ких протоколов
2	ПК-1	Способен понимать и применять в научно-исследовательской и прикладной деятельности современный математический аппарат, основные законы естествознания, современные языки программирования и программное обеспечение; операционные системы и	Основные математические задачи и алгоритмы, лежащие в основе работы криптографически х протоколов	Решать основные математические задачи и разрабатывать алгоритмы, лежащие в основе работы криптографически х протоколов	Способностью понимать и применять в научно-исследовательс кой и прикладной деятельности современный математический

		сетевые технологии			аппарат, лежащий в основе криптографических протоколов

2. Структура и содержание дисциплины

2.1 Распределение трудоемкости дисциплины по видам работ

Общая трудоемкость дисциплины составляет 3 зач.ед. (108 часов), их распределение по видам работ представлено в таблице.

Вид учебной работы		Всего часов	Семестры (часы)			
			8			
Контактная работа, в том числе:		48,3	48,3			
Аудиторные занятия (всего):		42	42			
Занятия лекционного типа		14	14			
Лабораторные занятия		28	28			
Занятия семинарского типа (семинары, практические занятия)		-	-			
Иная контактная работа:						
Контроль самостоятельной работы (КСР)		6	6			
Промежуточная аттестация (ИКР)		0,3	0,3			
Самостоятельная работа, в том числе:		6	6			
Курсовая работа		-	-			
Проработка учебного (теоретического материала)		3	3			
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		3	3			
Реферат		-	-			
Подготовка к текущему контролю		53,7	53,7			
Контроль:						
Подготовка к экзамену:		53,7	53,7			
Общая трудоемкость	**Час.**	**108**	**108**			
	В том числе контактная работа	**48,3**	**48,3**			
	Зач.ед.	**3**	**3**			

2.2 Структура дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы дисциплины, изучаемые в 8 семестре.

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная Работа
			Л	ПЗ	ЛР	СР
1	2	3	4	5	6	7

1	Криптографические протоколы и основные требования	7	2		4	1
2	Протоколы рукопожатия	7	2		4	1
3	Протоколы генерации ключей	9	2		6	1
4	Протоколы идентификации и аутентификации	11	4		6	1
5	Протоколы распределения ключей	7	2		4	1
6	Доказательства с нулевым разглашением секрета	7	2		4	1
	Итого:	48	14	-	28	6

2.3 Содержание разделов дисциплины

2.3.1 Занятия лекционного типа

№ раздела	Наименование раздела	Содержание раздела	Форма текущего Контроля
1	2	3	4
1	Криптографические протоколы и основные требования	Определение и свойства криптографических протоколов. Участники протокола. Общая классификация атак на криптографические протоколы. Компроментация криптографического протокола	ЛР
2	Протоколы рукопожатия	Протоколы аутентификации “запрос-ответ”, основанные на криптосистемах разных типов: классификация, примеры, стандартизация	ЛР
3	Протоколы генерации ключей	Основные подходы к конструированию стойких криптографических алгоритмов и протоколов в рамках концепции “доказательной безопасности”.	ЛР
4	Протоколы идентификации и аутентификации	Классификация протоколов идентификации и аутентификации. Протоколы аутентификации “запрос-ответ”, основанные на разных криптосистемах: классификация, примеры, стандартизация	ЛР
5	Протоколы распределения ключей	классификация протоколов распределения ключей (ПРК), основные и дополнительные свойства ПРК. Классификация ПРК, основанных на симметричных криптосхемах. Двусторонние протоколы.	ЛР
6	Доказательства с нулевым разглашением секрета	Интерактивные системы доказательства с нулевым разглашением знания: цель доказательства, общий принцип построения протокола, свойство нулевого разглашения знания, теоремы	ЛР

2.3.2 Занятия семинарского типа

Учебным планом не предусмотрены

2.3.3 Лабораторные занятия

№ работы	№ раздела дисциплины	Наименование лабораторных работ	Форма текущего Контроля
1	1	Производство и применение систем криптографической защиты информации	ЛР
2	1	Функции органа криптографической защиты информации. Обязанности пользователей СКЗИ.	ЛР
3	1	Требования к средствам защиты информации используемым в криптопрооколах	ЛР
4	2	Обязанности пользователей СКЗИ и криптопротоколов; Функции органа управления СКЗИ и использования криптопротоколов	ЛР
5	2	Механизмы контроля за организацией и обеспечением безопасности хранения обработки и передачи конфиденциальных данных на основе криптопротоколов	ЛР
6	3	Iротоколы распределения ключей с центром доверия, основанные на симметричных криптосхемах: протокол Needham-Schroeder	ЛР
7	3	Протоколы распределения ключей с центром доверия, основанные на симметричных криптосхемах: протокол протокол Kerberos	ЛР
8	3	Протоколы транспортировки ключей, рекомендованные стандартом X.509, Протокол транспортировки ключей Beller-Yacobi	ЛР
9	3	Протокол обмена ключами Диффи-Хеллмана, атаки на него	ЛР
10	4	Протокол обмена ключами MTI, атаки на него	ЛР
11	4	Протокол обмена ключами STS	ЛР
12	5	Каналы защищенной передачи информации: постановка задачи, классификация средств обеспечения конфиденциальности и аутентичности	ЛР
13	5	Протоколы распределения ключей с центром доверия, основанные на симметричных криптосхемах: протокол Otway-Rees	ЛР
14	6	Доказательства с нулевым разглашением знаний. Алгоритмы разделения секрета	ЛР

2.3.4 Примерная тематика курсовых работ (проектов)

Учебным планом не предусмотрены.

2.4. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа,

Для лиц с нарушениями слуха:

– в печатной форме,
– в форме электронного документа.
Для лиц с нарушениями опорно-двигательного аппарата:
– в печатной форме,
– в форме электронного документа,
Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии

Используемые интерактивные образовательные технологии:
- Компьютерные презентации и обсуждение.
- Разбор конкретных ситуаций (задач), тренинги по решению задач, компьютерные симуляции (программирование алгоритмов).

4. Оценочные и методические материалы

4.1 Оценочные средства для текущего контроля успеваемости и промежуточной успеваемости студентов

Фонд оценочных средств дисциплины состоит из средств текущего контроля выполнения контрольных работ, средств итоговой аттестации (экзамен в 8-ом семестре).

Оценка успеваемости осуществляется по результатам:

- выполнения контрольных работ;
- выполнения индивидуальных заданий;
- ответа на экзамене (для выявления знания и понимания теоретического материала дисциплины).

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводится в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:
– в печатной форме увеличенным шрифтом,
– в форме электронного документа.
Для лиц с нарушениями слуха:
– в печатной форме,
– в форме электронного документа.
Для лиц с нарушениями опорно-двигательного аппарата:
– в печатной форме,
– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Структура фонда оценочных средств для текущей и промежуточной аттестации

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства	
			Текущий	Промежуточная

			контроль	аттестация
1	Криптографические протоколы и основные требования	ОПК-5	ЛР,	Экзамен
2	Протоколы рукопожатия	ПК-1	ЛР	Экзамен
3	Протоколы генерации ключей	ПК-1	ЛР	Экзамен
4	Протоколы идентификации и аутентификации	ОПК-5	ЛР	Экзамен
5	Протоколы распределения ключей	ОПК-5	ЛР	Экзамен
6	Доказательства с нулевым разглашением секрета	ПК-1	ЛР	Экзамен

Показатели, критерии и шкала оценки сформированных компетенций

Компетенция	**Соответствие уровней освоения компетенции планируемым результатам обучения и критериям их оценивания**		
	Пороговый	**Базовый**	**Продвинутый**
	Оценка		
	Удовлетворительно /зачтено	Хорошо/зачтено	Отлично/зачтено
ОПК-5 – Способен инсталлировать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности	*Знает* – принципы работы основных криптопротоколов	*Знает* – принципы работы криптографических протоколов	*Знает* – недостатки современных криптографических протколов и тенденции их развития
	Умеет – инсталлировать программное обеспечение информационных систем с применением криптографических протоколов	*Умеет* – инсталлировать и сопровождать программное обеспечение информационных систем с применением криптографических протоколов	*Умеет* – применять методы и алгоритмы криптографических протоколов для разработки требуемого программного обеспечения
	Владеет – базовыми методами оценки эффективности работы криптографических протоколов	*Владеет* – Способностью оценивать эффективность работы криптографических протоколов	*Владеет* – способностью оценить эффективность применения криптографических протоколов в конкретных задачах разработки и сопровождения программного обеспечения
ПК-1 – Способен понимать и применять в научно-исследовательской и прикладной деятельности современный математический аппарат, основные	*Знает* – основные математические задачи, лежащие в основе работы криптографических протоколов	*Знает* – математические задачи и алгоритмы, лежащие в основе работы криптографических протоколов	*Знает* – современные тенденции развития математических основ криптоанализа
	Умеет – Решать основные математические задачи,	*Умеет* – Решать математические задачи и разрабатывать	*Умеет* – применять математический аппарат для оценки

законы естествознания, современные языки программирования и программное обеспечение; операционные системы и сетевые технологии	лежащие в основе работы криптографических протоколов	алгоритмы, лежащие в основе работы криптографических протоколов	эффективности и надежности применения криптографических протоколов для конкретных прикладных задач
	Владеет – Способностью понимать и применять в прикладной деятельности современные криптографические протоколы	*Владеет* – Способностью понимать и применять в прикладной деятельности современный математический аппарат, лежащий в основе криптографических протоколов	*Владеет* – Способностью понимать и применять в прикладной и научно-исследовательской деятельности современный математический аппарат, лежащий в основе криптографических протоколов

Типовые контрольные материалы или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы:

Образцы контрольных работ по основным разделам курса

Код оцениваемой компетенции –ПК-1, ОПК-5

1. Как преобразовать протокол аутентификации запрос-ответ на базе схемы открытого шифрования в протокол аутентичного распределения ключей? Приведите два примера: для протокола односторонней аутентификации и для протокола взаимной аутентификации.

2. Приведите описание процедуры восстановления секрета из схемы разделения секрета Шамира двумя способами: для случая, когда общее число участников равно 3, максимально допустимое количество утраченных (скомпроментированных) долей секрета равно 2, длина разделяемого секрета равно 128 битам.

3. Какими из основных свойств протоколов распределения ключей (неявная аутентификация ключа, подтверждение ключа, явная аутентификация) обладает протокол Kerberos? Какие практические задачи он позволяет решать?

4. Оцените вычислительную сложность (количество выполненных операций) и коммуникационную сложность (количество пересылок сообщений и объем передаваемых данных) протокола доказательства знания дискретного логарифма для каждого участника. Приведите пример такого задания параметров протокола, при котором вероятность обмана доказывающим проверяющего не превысит 2^{-30}.

5. Сравните по стойкости к различным видам атак два метода аутентификации по одноразовым паролям: метод Лэмпорта и последовательно обновляемые одноразовые пароли. Какие выводы о предпочтительности того или иного метода можно сделать?

Зачетно-экзаменационные материалы для промежуточной аттестации

Перечень вопросов, которые выносятся на экзамен в 8 семестре

1. Определение и свойства криптографических протоколов. Участники протокола. Общая классификация атак на криптографические протоколы. Компроментация криптографического протокола.
2. Критерии оценки стойкости криптографических алгоритмов и протоколов.
3. Характеристики вычислительно сложных задач теории чисел, возможности их применения в ассиметричной криптографии (задача факторизации и производные от нее задачи, задача дискретного логарифмирования и производные от нее задачи).
4. Парные отображения и их свойства. Вычислительно сложные задачи, основанные на парных отображениях.
5. Основные подходы к конструированию стойких криптографических алгоритмов и протоколов в рамках концепции “доказательной безопасности”.
6. Интерактивные системы доказательства: цель доказательства, общий принцип построения протокола, свойства полноты и корректности.
7. Интерактивные системы доказательства с нулевым разглашением знания: цель доказательства, общий принцип построения протокола, свойство нулевого разглашения знания, теоремы.
8. Классификация протоколов аутентификации. Атаки на протоколы с фиксированными паролями.
9. Протоколы аутентификации с одноразовыми паролями. Схема Лэмпорта.
10. Протоколы аутентификации “запрос-ответ”, основанные на симметричных криптосистемах: классификация, примеры, стандартизация (ISO/IEC 9798).
11. Протоколы аутентификации “запрос-ответ”, основанные на асимметричных криптосистемах: классификация, примеры, стандартизация (ISO/IEC 9798).
12. Протоколы аутентификации, основанные на доказательствах с нулевым разглашением знаний (на примере проокола Фиата-Шамира).
13. Общая классификация протоколов распределения ключей (ПРК), основные и дополнительные свойства ПРК.
14. Классификация ПРК, основанных на симметричных криптосхемах. Двусторонние протоколы (без центра доверия).
15. ПРК с центром доверия, основанные на симметричных криптосхемах:
протокол Needham-Schroeder, протокол Kerberos.
16. ПРК с центром доверия, основанные на симметричных криптосхемах: протокол Otway-Rees, атаки на него.
17. Классификация ПРК, основанных на симметричных криптосхемах. Протокол транспортировки ключей Needham-Schroeder с использованием схем открытого шифрования.
18. Протоколы транспортировки ключей, рекомендованные стандартом X.509.
19. Протокол транспортировки ключей Beller-Yacobi.
20. Протокол обмена ключами Диффи-Хеллмана, атаки на него.
21. Протокол обмена ключами MTI, атаки на него.
22. Протокол обмена ключами STS.
23. Каналы защищенной передачи информации: постановка задачи, классификация средств обеспечения конфиденциальности и аутентичности.
24. Криптографические механизмы в спецификации SSH: аутентичное распределение ключей, защита передаваемых по каналу сообщений.
25. Криптографические механизмы в спецификации SSL/TLS: аутентичное распределение ключей, защита передаваемых по каналу сообщений.
26. Криптографические механизмы в спецификации IPSec: аутентичное распределение ключей, защита передаваемых по каналу сообщений.

27. Схема проверяемого разделения секрета Фельдмана.
28. Схема проверяемого разделения секрета Педерсена.

Критерии оценивания к экзамену

Оценка «отлично»: точные формулировки алгоритмов, теорем и правильные доказательства; точные определения математических объектов и ясные и правильные определения объектов, характеризующихся неформализованными понятиями.

Оценка «хорошо»: при ответе на один вопрос даны точные формулировки алгоритмов, теорем и правильные доказательства; точные определения математических объектов и ясные и правильные определения объектов, характеризующихся неформализованными понятиями; при ответе на второй вопрос имеются неточности формулировки алгоритмов, теорем или пробелы в правильных доказательствах; недостаточно точные определения математических объектов или неясные и не совсем правильные определения объектов, характеризующихся неформализованными понятиями.

Оценка «удовлетворительно»: при ответе на оба вопроса имеются неточности формулировки алгоритмов, теорем или пробелы в правильных доказательствах; недостаточно точные определения математических объектов или неясные и не совсем правильные определения объектов, характеризующихся неформализованными понятиями.

Оценка «неудовлетворительно»: отсутствует ответ хотя бы на один из вопросов или имеются существенные неточности в формулировках алгоритмов, теорем, приведены неправильные доказательства; неверные определения математических объектов и неправильные определения объектов, характеризующихся неформализованными понятиями.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

5.1 Основная литература

1. Ищукова, Е.А. Криптографические протоколы и стандарты : учебное пособие / Е.А. Ищукова, Е.А. Лобова ; Министерство образования и науки РФ, Южный федеральный университет, Инженерно-технологическая академия. - Таганрог : Издательство Южного федерального университета, 2016. - 80 с. : ил. - Библиогр. в кн. - ISBN 978-5-9275-2066-4 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=493059

2. Информационная безопасность и защита информации [Текст] : учебное пособие для студентов вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - 5-е изд., стер. - М. : Академия, 2011. - 331 с. : ил. - (Высшее профессиональное образование . Информатика и вычислительная техника) (Учебное пособие). - Библиогр.: с. 327-328. . (36 экз. в библиотеке КубГУ).

5.2 Дополнительная литература

1. Алгебраические задачи криптографии [Текст] : практикум / [сост. С. В. Нагорный] М-во образования и науки Рос. Федерации ; КубГУ. - Краснодар : [КубГУ], 2005. - 26 с. (29 экз. в библиотеке КубГУ).

2. Лапонина, О.Р. Криптографические основы безопасности / О.Р. Лапонина. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 244 с. [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429092

3. Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации [Текст] : учебное пособие для студентов вузов /. - М. : Горячая линия-Телеком , 2005. - 229 с. . (10 экз. в библиотеке КубГУ).

4. Лапонина О. Р. [под ред. В. А. Сухомлина] Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия [Текст] : учебное пособие для студентов вузов / - 2-е изд., испр. - М. : Интернет-Университет Информационных Технологий : БИНОМ. Лаборатория знаний , 2007. - 531 с. (10 экз. в библиотеке КубГУ).

6. Методические указания для обучающихся по освоению дисциплины (модуля)

По курсу предусмотрено проведение лекционных занятий, на которых дается основной систематизированный материал, и лабораторных работ, во время которых закрепляется теоретический материал решением задач.

На лабораторных занятиях проводится стандартная работа по решению задач по дискретной математике. По отдельным темам студентам поручается подготовить презентации и выступить с докладами на занятиях.

Важнейшим этапом курса является самостоятельная работа по дисциплине с использованием указанных литературных источников.

Для лучшего освоения дисциплины при ответах на ЛР студент должен ответить на несколько вопросов из лекционной части курса.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья

7. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

7.1 Перечень информационных технологий.

– Проверка домашних заданий и консультирование посредством электронной почты.
- Использование электронных презентаций при проведении лекций и практических занятий

7.2 Перечень необходимого программного обеспечения

MSOffice.

8. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Лекционная аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) и соответствующим программным обеспечением (ПО) PowerPoint. ауд. 129, 131, А305.
2.	Лабораторные занятия	Аудитории для лабораторных занятий, оборудованные досками.
3.	Групповые (индивидуальные) консультации	Аудитории для лабораторных занятий, оборудованные досками.
4.	Текущий контроль, промежуточная аттестация	Аудитория, приспособленная для письменного ответа при промежуточной аттестации.
5.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета.