МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Факультет компьютерных технологий и прикладной математики
Кафедра вычислительных технологий

УТВЕРЖДАЮ
Проректор по учебной работе, качеству образования – первый проректор
_____ Хагуров Т.А.
подпись

«__30___» ___мая____ 2025г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.О.28 «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

Программа подготовки *академический бакалавриат*

Форма обучения *очная*

Квалификация выпускника *бакалавр*

Краснодар
2025

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):

Руденко О.В. доцент , канд.тех.наук
Ф.И.О. , должность, ученая степень, ученое звание — подпись

Рабочая программа дисциплины «Криптографические протоколы» утверждена назаседании кафедры Вычислительных технологий

протокол № 7 «3 » мая 2025 г.

и.о.заведующего кафедрой (разработчика) Еремин А.А.
(фамилия, инициалы — подпись

Утверждена на заседании учебно-методической комиссии факультета Компьютерных Технологий и Прикладной Математики
протокол № 4 от «23 » мая 2025 г

Председатель УМК факультета Коваленко А.В.

фамилия, инициалы — подпись

Рецензенты:

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

Авакимян Н.Н., доцент ККТиС КубГАУ , к.ф.-м.н., доцент

1. Цели и задачи освоения дисциплины

1.1 Цель освоения дисциплины

Учебная дисциплина «Криптографические протоколы» предназначена для профессиональной разработки с применением криптографической защиты.

Целью курса «Криптографические протоколы» является изучение математических основ криптологии, основных криптоалгоритмов, стандартных криптопротоколов и аспектов их применения.

1.2 Задачи дисциплины

В результате освоения данной компетенции студент должен:

знать основные блоки симметричных шифров, математические аспекты безопасности шифров, стандарты и ГОСТы криптопротоколов.

уметь построить программную реализацию существующих криптоалгоритмов средствами произвольного языка, построить криптопротокол обмена информацией с помощью встроенных библиотек, построить модель реализации заданной атаки на криптопротокол;

владеть навыками свободного обращения с программными реализациями криптоалгоритмов; навыками построения архитектуры защищенных программных систем с применением существующих протоколов.

1.3. Место дисциплины (модуля) в структуре образовательной программы

Курс «Криптографические протоколы» относится к части, формируемой участниками образовательных отношений блока Б1 Дисциплины (модули) и является обязательной.

Для изучения дисциплины студент должен владеть знаниями, умениями и навыками по дисциплинам: Алгебра, Дискретная математика, Теория графов и ее приложения, Комбинаторный анализ, Информационная безопасность, Программирование в компьютерных сетях, Интерпретируемые языки программирования, Платформо-независимое программирование, с которыми дисциплина связана логически и содержательно-методически.

Дисциплина является предшествует изучению дисциплин: «Преддипломная практика», «Защита выпускной квалификационной работы».

1.4 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы.

Изучение данной учебной дисциплины направлено на формирование у обучающихся универсальных/ общепрофессиональных/ профессиональных компетенций (УК/ОПК/ПК):

Код и наименование индикатора	Результаты обучения по дисциплине *(знает, умеет, владеет (навыки и/или опыт деятельности))*
ОПК-5 Способен инсталлировать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности	
ОПК-5.1. Знает методику установки и администрирования информационных систем и базданных. Знаком с содержанием Единого реестра российских программ.	современные подходы к организации сложных криптосистем; основные международные стандарты, регламентирующие применение криптографических методов защиты информации
ОПК-5.2. Умеет реализовывать техническое сопровождение информационных систем и баз данных.	анализировать текущее состояние ИБ на предприятии с целью разработки требований к средствам криптографической защиты информации (СКЗИ)

Код и наименование индикатора	Результаты обучения по дисциплине *(знает, умеет, владеет (навыки и/или опыт деятельности))*
ОПК-5.3. Имеет практический опыт участия в научных студенческих конференциях, очных,виртуальных, заочных обсуждениях научных проблем в области информационных технологий.	навыками решения задач количественной оценки стойкости и производительности криптографических протоколов
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 сетевые технологии	
ПК-1.1. Знает основы научно-исследовательской деятельности в области информационных технологий, имеет научные знания в теории информационных систем.	основные задачи и понятия криптографии; требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры
ПК-1.2. Умеет применять полученные знания в области фундаментальных научных основ теории информации и решать стандартные задачи в собственной научно-исследовательской деятельности.	применять математические методы исследования моделей шифров
ПК-1.3. Имеет практический опыт научно- исследовательской деятельности в области информационных технологий.	навыками использования типовых криптографических алгоритмов; навыками использования ЭВМ в анализе простейших шифров

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости 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	Форма обучения
		очная
		Семестры (часы)
		8
Контактная работа, в том числе:		
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)		2	2
Промежуточная аттестация (ИКР)		0,3	0,3
Самостоятельная работа, в том числе:		**10**	**10**
Курсовая работа		–	–
Проработка учебного (теоретического) материала		2	2
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		5	5
Реферат		–	–
Подготовка к текущему контролю		3	3
Контроль:		**экзамен**	**экзамен**
Подготовка к экзамену		53,7	53,7
Общая трудоёмкость	**час.**	**108**	**108**
	в том числе контактная работа	**44,3**	**44,3**
	зач. ед.	**3**	**3**

2.2 Содержание дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы дисциплины, изучаемые в _8_ семестре (очная форма).

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1	Математические основы криптологии.	21	6	–	10	5
2	Криптоалгоритмы.	17	4	–	10	3
3	Криптопротоколы	14	4	–	8	2
4	Подготовка к экзамену	53,7				
5	ИКР	0,3				
6	КСР	2				
7	Общая трудоемкость по дисциплине*:*	**108**	**14**	–	**28**	**10**

Примечание: Л – лекционные занятия, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

2.3 Содержание разделов (тем) дисциплины

2.3.1 Занятия лекционного типа

№ раз-дела	Наименование раздела(темы)	Содержание раздела (темы)	Форма текущего контроля
1	2	3	4
1	Математические основы криптологии.	Системы вычетов. НОД, функция Эйлера, основная теорема арифметики. Мультипликативная инверсия, расширенный алгоритм Евклида. Малая теорема Ферма, формула Эйлера, примитивный элемент поля. Решение сравнений первой степени. Китайская теорема об остатках. Алгоритмы проверки на простоту. Тест Миллера-Рабина. Задача факторизации числа. Эллиптические кривые.	ЛР
2	Криптоалгоритмы.	Типы атак на криптосистемы. Понятие стойкости	ЛР

		шифра по Шеннону. Совершенные шифры. Алгоритм Блюм-Блюм-Шуба. Регистр сдвига. М-последовательность, нелинейный усложнитель. Вихрь Мерсена. Тесты NIST. Тесты DIE HARD. Общие подходы к построению блочных симметричных шифров. Обратимые и необратимые операции, классификация блочных шифров. Шифры Фейстеля. Шифр DES. Шифр AES. SubBytes, AddRoundKey. Криптография в эллиптических кривых	
3	Криптопротоколы	Понятие хэш-функции. Понятие коллизий. Понятие криптографически стойкой хэш функции, классификация. MD5. Sha-2 . Стрибог. Построение хэш функций на симметричных алгоритмах. Протоколы построения. Whirpool. ЭЦП. ГОСТ 34.10-2018.	ЛР

Защита лабораторной работы (ЛР), выполнение курсового проекта (КП), курсовой работы (КР), расчетно-графического задания (РГЗ), написание реферата (Р), эссе (Э), коллоквиум (К), тестирование (Т) и т.д.

2.3.2 Занятия семинарского типа

Учебным планом не предусмотрены.

2.3.3 Лабораторные занятия

№ работы	Наименование лабораторных работ	Форма текущего контроля
1	Элементы теории чисел. Решение сравнений	ЛР
2	Кольцо многочленов. Поля Галуа.	ЛР
3	NP-полные задачи теории чисел.	ЛР
4	Группы точек эллиптических кривых.	ЛР
5	Математические основы криптологии	ЛР
6	ПСП	ЛР
7	Симметричные шифры	ЛР
8	Ассиметричные шифры	ЛР
9	Применение шифров	ЛР
10	ХЭШ/ЭЦП	ЛР
11	Электронная подпись на основе шифрсистем с открытыми ключами.	ЛР
12	Электронные подписи на основе симметричных криптосистем.	ЛР
13	Распределение ключей	ЛР
14	Криптоалгоритмы и криптопротоколы	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)

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы

1	2	3
1	Индивидуальное задание	Источники основной и дополнительнойлитературы

Учебно-методические материалы для самостоятельной работы обучающихся и 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, применяемые при освоении дисциплины (модуля)

При проведении занятий по дисциплине используются следующие образовательные технологии:

– технология разноуровневого обучения (дифференцированное обучение);

– технология коллективного взаимодействия (организованный диалог, коллективный способ обучения).

Технология адаптивного обучения (индивидуализированное обучение).

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
6	Л	Компьютерные презентации и обсуждение	14
	ЛР	Разбор конкретных ситуаций (задач), тренинги по решению задач, компьютерные симуляции (программирование алгоритмов)	28
Итого:			42

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Методы поисковой оптимизации».

4.1 Фонд оценочных средств для проведения текущего контроля

Фонд оценочных средств дисциплины состоит из средств текущего контроля выполнения заданий, лабораторных работ, средств итоговой аттестации (экзамен в 6 семестре).

Оценка успеваемости осуществляется по результатам:

- выполнения лабораторных работ;
- ответов на теоретические вопросы при сдаче лабораторных работ;
- 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 проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) 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 оценочных средств для текущей и промежуточной аттестации

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1.	Математические основы криптологии.	ОПК-5, ПК-1	ЛР	Вопросы 1-11
2.	Криптоалгоритмы.	ОПК-5, ПК-1	ЛР	Вопросы 12-29
3.	Криптопротоколы	ОПК-5, ПК-1	ЛР	Вопрос 30-36

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Код и наименование индикатора	Результаты обучения	Наименование оценочного средства	
			Текущий контроль	Промежу-точная аттестация
1	ОПК-5.1. Знает методику установки и администрирования информационных систем и баз данных. Знаком с содержанием Единого реестра российских программ.	современные подходы к организации сложных криптосистем; основные международные стандарты, регламентирующие применение криптографических методов защиты информации	опрос по теме, лабораторная работа	Вопросы на зачет 1-36
2	ОПК-5.2. Умеет реализовывать техническое сопровождение информационных систем и баз данных.	анализировать текущее состояние ИБ на предприятии с целью разработки требований к средствам криптографической защиты информации (СКЗИ)	опрос по теме, лабораторная работа	Вопросы на зачет 1-36

3	ОПК-5.3. Имеет практический опыт участия в научных студенческих конференциях, очных,виртуальных, заочных обсуждениях научных проблем в области информационных технологий	навыками решения задач количественной оценки стойкости и производительности криптографических протоколов	опрос по теме, лабораторная работа	Вопросы на зачет 1-36
4	ПК-1.1. Знает основы научно-исследовательской деятельности в области информационных технологий, имеет научные знания в теории информационных систем.	основные задачи и понятия криптографии; требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры	опрос по теме, лабораторная работа	Вопросы на зачет 1-36
5	ПК-1.2. Умеет применять полученные знания в области фундаментальных научных основ теории информации и решать стандартные задачи в собственной научно-исследовательской деятельности.	применять математические методы исследования моделей шифров	опрос по теме, лабораторная работа	Вопросы на зачет 1-36
6	ПК-1.3. Имеет практический опыт научно-исследовательской деятельности в области информационных технологий.	навыками использования типовых криптографических алгоритмов; навыками использования ЭВМ в анализе простейших шифров	опрос по теме, лабораторная работа	Вопросы на зачет 1-36

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

№ работы	№ раздела дисциплины	Наименование лабораторных работ
1	1	Элементы теории чисел. Решение сравнений.(ОПК-5, ПК-1)
2		Кольцо многочленов. Поля Галуа. .(ОПК-5, ПК-1)
3		NP-полные задачи теории чисел. .(ОПК-5, ПК-1)
4		Группы точек эллиптических кривых. .(ОПК-5, ПК-1)
5		Математические основы криптологии.(ОПК-5, ПК-1)
6	2	ПСП.(ОПК-5, ПК-1)
7		Симметричные шифры.(ОПК-5, ПК-1)
8		Ассиметричные шифры.(ОПК-5, ПК-1)
9		Применение шифров.(ОПК-5, ПК-1)
10		ХЭШ/ЭЦП.(ОПК-5, ПК-1)
11	3	Электронная подпись на основе шифрсистем с открытыми ключами .(ОПК-5, ПК-1)
12		Электронные подписи на основе симметричных криптосистем.(ОПК-5, ПК-1)
13		Распределение ключей .(ОПК-5, ПК-1)
14		Криптоалгоритмы и криптопротоколы.(ОПК-5, ПК-1)

Отчет должен содержать:
- постановку задачи;
- краткое описание проделанной работы;
- список использованной литературы.

Зачетно-экзаменационные материалы для промежуточной аттестации (экзамен/зачет)

1. Кольцо, поле. (ОПК-5, ПК-1)
2. Системы вычетов. (ОПК-5, ПК-1)
3. НОД, функция Эйлера, основная теорема арифметики. (ОПК-5, ПК-1)
4. Малая теорема Ферма, формула Эйлера, примитивный элемент поля. (ОПК-5, ПК-1)
5. Диофантовы уравнения. Решение простейших диофантовых уравнений 1степени. (ОПК-5, ПК-1)
6. Решение сравнений первой степени. (ОПК-5, ПК-1)
7. Китайская теорема об остатках, решение системы сравнений.(ОПК-5, ПК-1)
8. Алгоритмы проверки на простоту. Вероятностные алгоритмы. (ОПК-5, ПК-1)
9. Тест Миллера-Рабина. Общий подход к проверке числа на простоту.(ОПК-5, ПК-1)
10. Задача факторизации числа, метод Ферма, методы Полларда. (ОПК-5, ПК-1)
11. Точки эллиптических кривых. Операции, группа точек.(ОПК-5, ПК-1)
12. Типы атак на криптосистемы. (ОПК-5, ПК-1)
13. Понятие стойкости шифра по Шеннону. Совершенные шифры.Классификация шифров. (ОПК-5, ПК-1)
14. Криптоалгоритмы и криптопротоколы.Классические шифры. (ОПК-5, ПК-1)
15. Представление данных и операции над ними в современных криптосистемах. (ОПК-5, ПК-1)
16. Алгоритм Блюм-Блюм-Шуба. (ОПК-5, ПК-1)
17. Регистр сдвига. (ОПК-5, ПК-1)
18. М-последовательность, нелинейный усложнитель.(ОПК-5, ПК-1)
19. Вихрь Мерсена. (ОПК-5, ПК-1)
20. Тесты NIST. (ОПК-5, ПК-1)
21. Тесты DIE HARD. (ОПК-5, ПК-1)
22. Общие подходы к построению блочных симметричных шифров. (ОПК-5, ПК-1)
23. Шифры Фейстеля. (ОПК-5, ПК-1)
24. Шифр DES. Параметры и общая структура.(ОПК-5, ПК-1)
25. Шифр DES. Расширение ключей. (ОПК-5, ПК-1)
26. Шифр DES. Уязвимости. TRIPLE DES. (ОПК-5, ПК-1)
27. Шифр AES. Параметры и общая структура. (ОПК-5, ПК-1)
28. Шифр AES. Структура раунда. SubBytes, AddRoundKey. (ОПК-5, ПК-1)
29. Криптография в эллиптических кривых. (ОПК-5, ПК-1)
30. Понятие хэш-функции. Понятие коллизий. (ОПК-5, ПК-1)
31. Понятие криптографически стойкой хэш функции, классификация Хэшей. (ОПК-5, ПК-1)
32. MD5. (ОПК-5, ПК-1)
33. Sha-2. (ОПК-5, ПК-1)
34. Стрибог. (ОПК-5, ПК-1)
35. ЭЦП. Терминология. Общие принципы и протоколы применения.(ОПК-5, ПК-1)
36. ГОСТ 34.10-2018. (ОПК-5, ПК-1)

4.2 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

4.2.1 Методические рекомендации к сдаче зачета

Оценка успеваемости осуществляется по результатам:

- выполнения лабораторных работ;
- ответов на теоретические вопросы при сдаче лабораторных работ;
- ответа на зачете (для выявления знания и понимания теоретического материала дисциплины).

4.2.2 Критерии оценивания результатов обучения

Оценка	Критерии оценивания по экзамену
Высокий уровень «5» (отлично)	оценку «отлично» заслуживает студент, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все задания, предусмотренные учебным планом на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы.
Средний уровень «4» (хорошо)	оценку «хорошо» заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в основном сформировал практические навыки.
Пороговый уровень «3» (удовлетворительно)	оценку «удовлетворительно» заслуживает студент, частично с пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические навыки не сформированы.
Минимальный уровень «2» (неудовлетворительно)	оценку «неудовлетворительно» заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы.

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

5.1 Основная литература

1. Торстейнсон, П. Криптография и безопасность в технологии .NET / П. Торстейнсон, Г.А. Ганеш ; под ред. С. М. Молявко ; пер. с англ. В. Д. Хорева. - 4-еизд. - Москва : Лаборатория знаний, 2020. - 428 с. - URL: https://e.lanbook.com/book/151552 (дата обращения: 13.04.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-00101-700-4. - Текст : электронный.

2. Алгебра и теория чисел для криптографии : учебное пособие / Л. М. Мартынов. - 3-е изд., стер. - Санкт-Петербург : Лань, 2024. - 456 с. - URL: https://e.lanbook.com/book/362942 (дата обращения: 19.02.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-48774-5. - Текст : электронный.

3. 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 : Юрайт, 2022. - 473 с. - URL: https://urait.ru/bcode/489242 (дата обращения: 26.01.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-534-12474-3. - Текст : электронный.

4. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. - Москва : Юрайт, 2022. - 349 с. - URL: https://urait.ru/bcode/489919 (дата обращения: 30.05.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-534-02883-6. - Текст : электронный.

5.2 Дополнительная литература

1. Математические методы защиты информации : учебное пособие для вузов / С. М. Рацеев. - Санкт-Петербург : Лань, 2022. - 544 с. - URL: https://e.lanbook.com/book/193323 (дата обращения: 15.12.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-8114-8589-5. - Текст : электронный.

2. Лапонина, О.Р. Криптографические основы безопасности : учебное пособие / О.Р. Лапонина. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 244 с. - URL: https://biblioclub.ru/index.php?page=book&id=429092 (дата обращения: 04.03.2021). - Режим доступа: для авториз. пользователей. - ISBN 5-9556-00020-5. - Текст : электронный.

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

По курсу предусмотрено проведение лекционных занятий, на которых дается основной систематизированный материал, лабораторных работ, контрольной работы, экзамена.

Важнейшим этапом курса является самостоятельная работа по дисциплине с использованием указанных литературных источников и методических указаний автора курса.

Виды и формы СР, сроки выполнения, формы контроля приведены выше в данном документе.

Для лучшего освоения дисциплины при защите 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. Материально-техническое обеспечение по дисциплине (модулю)

№	Вид работ	Наименование учебной аудитории, ее оснащенность оборудованием и техническими средствами обучения
1.	Лекционные занятия	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения
2.	Лабораторные занятия	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, компьютерами, проектором, программным обеспечением
3.	Групповые (индивидуальные) консультации	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, компьютерами, программным обеспечением
4.	Текущий контроль, промежуточная аттестация	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, компьютерами, программным обеспечением
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.

Примечание: конкретизация аудиторий и их оснащение определяется ОПОП.