МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Факультет компьютерных технологий и прикладной математики

подпись

«30» мая 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) Б1.О.33«СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ПЕРЕДАЧИ И ЗАЩИТЫ ИНФОРМАЦИИ»

Направление подготовки/специальность *09.03.03* Прикладная информатика

Направленность (профиль) / специализация *Искусственный интеллект и машинное обучение*

Форма обучения *очная*

Квалификация бакалавр

Краснодар 2025

Рабочая программа дисциплины «Современные технологии передачи и защиты информации» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки / специальности *09.03.03* Прикладная информатика

Программу составил(и):

Осипян В. О. проф., д. физ.-мат. наук, доцент

Рабочая программа дисциплины «Современные технологии передачи и защиты информации» утверждена на заседании кафедры анализа данных и искусственного интеллекта № 4 от «23» мая 2025 г.

Заведующий кафедрой
А. В. Коваленко

Рабочая программа обсуждена на заседании кафедры анализа данных и искусственного интеллекта протокол №8 от «18» мая 2023 г.
Заведующий кафедрой (разработчика)
А. В. Коваленко

Председатель УМК факультета Коваленко А.В

Рецензенты:
Шапошникова Татьяна Леонидовна.
Доктор педагогических наук, кандидат физико-математических наук, профессор. Почетный работник высшего профессионального образования РФ. Директор института фундаментальных наук (ИФН) ФГБОУ ВО «КубГТУ».

Марков Виталий Николаевич.
Доктор технических наук. Профессор кафедры информационных систем и программирования института компьютерных систем и информационной безопасности (ИКСиИБ) ФГБОУ ВО «КубГТУ».

1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

1.1 Цель освоения дисциплины

Цель освоения дисциплины «Современные технологии передачи и защиты информации» – формирование у студентов основ знаний об информационной безопасности, роли и внедрении информации в современном обществе; изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

Содержательное наполнение дисциплины обусловлено общими задачами в подготовке бакалавров. Научной основой для построения программы данной дисциплины является теоретико-прагматический подход в обучении. Студент должен осуществлять профессиональную деятельность и уметь решать задачи, соответствующие программе дисциплины.

1.2 Задачи дисциплины

Задачей дисциплины является изложение теории информационной безопасности и практики применения алгоритмов криптозащиты. Основные задачи дисциплины на основе системного подхода:

- Описать проблемную область информационной безопасности.
- Дать описание практического применения теории конечных полей в теории защиты информации.
- Расширить понятия о способах защиты информации.
- Расширить понятия о методах построения современных программных систем.
- Дать навыки практической работы с методами защиты информации.
- Дать навыки практической работы по решению задач идентификации.
- Дать навыки практической работы по решению задач цифровой подписи.

Научной основой для построения программы данной дисциплины является теоретико-прагматический подход в обучении.

1.3 Место дисциплины в структуре образовательной программы

Дисциплина «Современные технологии передачи и защиты информации» входит в базовую часть Блока 1 «Дисциплины (модули)» дисциплин, формирующих знания и навыки в области разработки современного программного обеспечения. Дисциплина опирается на знания в области дискретной математики, математической логики, программирования, базы данных. Дисциплина расширяет знания студентов в области создания программных систем, защиты данных и знаний.

Дисциплина тесно связана с дисциплинами «Математическое моделирование информационных систем и процессов», «Высокопроизводительные технологии программирования».

К результатам обучения относятся: фундаментальная подготовка по основам профессиональных знаний; способность понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе; соблюдение основных требований информационной

безопасности, в том числе защиты государственной тайны владение основными методами, способами и средствами получения, хранения, переработки информации, имеет навыки работы с компьютером как средством управления информацией способность к анализу и синтезу; способность определения общих форм, закономерностей, инструментальных средств данной дисциплины; умение

понять поставленную задачу

умение грамотно пользоваться языком предметной области;

умение извлекать полезную научно-техническую информацию из электронных библиотек, реферативных журналов, сети Интернет знание математических

основ информатики как науки

знание проблемы современной информатики, ее категории и связи с другими научными дисциплинами; знание содержания, основных этапов и тенденции развития

программирования,

математического обеспечения и информационных технологий.

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

Студент должен осуществлять профессиональную деятельность и уметь решать задачи, соответствующие программе дисциплины.

Знать	1) области применения задач информационной безопасности; 2) стандарты шифрования; 3) методы защиты информации; 4) области применения различных методов информационной безопасности;
	5) этапы, методы и инструментальные средства информационной безопасности. 6) принципы построения и функционирования систем информационной безопасности; 7) способностью разрабатывать и анализировать концептуальные и теоретические модели 8) классификацию шифров; 9) основы организации идентификации и цифровой подписи; 10) принципы построения и применения паролей; 11) правовые и этические последствия при получении доступа к информации не санкционированным лица

Уметь	12) проводить анализ и определять оптимальный метод защиты информации; 13) формировать требования к предметно-ориентированной системе информационной безопасности и определять возможные пути их выполнения; 14) анализировать модели шифрования при организации защиты данных 15) формулировать и решать задачи организации процесса цифровой подписи; 16) формулировать и решать задачи организации процесса идентификации; 17) реализовать на языке программирования заданный метод защиты информации; 18) использовать математический аппарат определяющий шифр; 19) решать задачи анализа шифра; 20) оценить последствия при компрометации ключа или шифра
Владеть	21) методологиями и парадигмами построение систем информационной безопасности; 22) методами проектирования систем защиты информации; 23) методами построения алгоритмов анализа; 24) методами построения систем идентификации; 25) методами определения требований и состава средств, мероприятий по системе информационной безопасности систем; 26) навыками оценки правовых и этических компрометации данных 27) методами определения и создания шифра

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
1.	УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	1, 2, 3, 5, 6, 7,8 9, 10	11, 12, 13, 19, 20	25, 26
2.	ПК-6	Способен моделировать прикладные (бизнес) процессы и предметную область.	2, 4, 5, 6, 10	12, 13, 20	22, 25,26

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 2 зач.ед. (72 часов), их распределение по видам работ представлено в таблице:

Вид учебной работы		Всего часов	Семестры(часы)			
			8			
Контактная работа, в том числе:		30,2	30,2			
Аудиторные занятия (всего):		28	28			
Занятия лекционного типа		14	14			
Лабораторные занятия		14	14			
Иная контактная работа:		2,2	2,2			
Промежуточная аттестация (ИКР)		0,2	0,2			
Контроль самостоятельной работы (КСР)		2	2			
Самостоятельная работа, в том числе:		41,8	41,8			
Выполнение индивидуальных заданий		41,8	41,8			
Подготовка к текущему контролю		-				
Контроль:						
Подготовка к экзамену		-				
Общая трудоемкость	**час.**	**72**				
	в том числе контактная работа	**30,2**				
	зач. ед	**2**				

Процедура промежуточной аттестации проходит в форме экзамена.

2.2 Структура дисциплины: Распределение видов учебной работы и их трудоемкости по разделам дисциплины. Разделы дисциплины, изучаемые в 1 семестре (очная форма). Вид промежуточной аттестации: экзамен.

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа		Внеаудиторная работа	
			Л	ЛР	СР	контроль
1.	Базовые понятия и история развития информационной безопасности.	2	2	2	4	
2	Конечные поля. Многочлены над конечным полем. Последовательности над конечным полем.	2	2	2	6	
3	Шифры замены. Шифры перестановки. Шифры гаммирования.	2	2	2	8	
4	Блочные системы шифрования.	2	2	2	8	
5	Поточные системы шифрования.	3	3	3	8	
6	Идентификация. Цифровые подписи.	3	3	3	7,8	
7	Промежуточная аттестация (ИКР)	0,2				0,2
8	Контроль самостоятельной работы (КСР)	2				2
9	Итого по дисциплине:	72	14	14	41,8	2,2

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, СР – самостоятельная работа студента

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа.

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1.	Базовые понятия и история развития информационной безопасности.	Защита информации. Угрозы информационной безопасности. Угрозы информационной безопасности.	собеседование
2.	Конечные поля. Многочлены над конечным полем. Последовательности над конечным полем.	Конечные поля. Характеристика поля. Мультипликативная группа конечного поля. Неприводимые многочлены. Порядок многочлена над конечным полем. Последовательности над конечным полем. Псевдослучайные последовательности и их применение. Линейные рекуррентные последовательности над конечным полем. Линейные рекуррентные последовательности как псевдослучайные последовательности.	собеседование, индивидуальное задание

3.	Шифры замены. Шифры перестановки. Шифры гаммирования.	Математическая модель шифра замены. Классификация шифров замены. Поточные шифры простой замены. Криптоанализ поточного шифра простой замены. Блочные шифры простой замены. Многоалфавитные шифры замены. Дисковые многоалфавитные шифры замены. Шифры перестановки. Маршрутные перестановки. Элементы криптоанализа шифров перестановки. Табличное гаммирование. О возможности восстановления вероятностей знаков гаммы.	собеседование, индивидуальное задание
4.	Блочные системы шифрования.	Блочные системы шифрования. Принципы построения блочных шифров. Американский стандарт шифрования данных DES. Стандарт шифрования данных ГОСТ 28147-89. Методы	собеседование, индивидуальное задание
		анализа алгоритмов блочного шифрования	
5.	Поточные системы шифрования.	Поточные системы шифрования. Шифрсистема A5. ШифрсистемаГиффорда. Линейные регистры сдвига. Алгоритм Берлекемпа—Месси. Методы анализа поточных шифров.	собеседование, индивидуальное задание
6.	Идентификация. Цифровые подписи.	Идентификация. Фиксированные пароли. Парольные фразы. Атаки на фиксированные пароли. Одноразовые пароли. Протоколы с нулевым разглашением. Атаки на протоколы идентификации. Цифровые подписи. Цифровая подпись Фиата-Шамира. Цифровая подпись ЭльГамаля. Одноразовые цифровые подписи.	собеседование, индивидуальное задание

2.3.2 Занятия семинарского типа.

Не предусмотрены

2.3.3 Лабораторные занятия.

№	Наименование лабораторных работ	Форма текущего контроля
1.	Основные шифры.	индивидуальное задание
2.	Стойкость шифров.	индивидуальное задание
3.	Конечные поля. Характеристика поля. Мультипликативная группа конечного поля.	индивидуальное задание
4.	Неприводимые многочлены. Порядок многочлена над конечным полем. Последовательности над конечным полем.	индивидуальное задание

5.	Последовательности над конечным полем. Псевдослучайные последовательности и их применение. Линейные рекуррентные последовательности над конечным полем. Линейные рекуррентные последовательности как псевдослучайные последовательности.	индивидуальное задание
6.	Математическая модель шифра замены. Поточные шифры простой замены. Блочные шифры простой замены.	индивидуальное задание
7.	Многоалфавитные шифры замены. Шифры перестановки. Маршрутные перестановки.	индивидуальное задание
8.	Табличное гаммирование.	индивидуальное задание
9.	Принципы построения блочных шифров.	индивидуальное задание
10.	Американский стандарт шифрования данных DES и его модификации.	индивидуальное задание
11.	Стандарт шифрования данных ГОСТ 28147-89. Методы анализа алгоритмов блочного шифрования	индивидуальное задание
12.	Поточные системы шифрования.	индивидуальное задание
13.	Линейные регистры сдвига.	индивидуальное задание
14.	Методы анализа поточных шифров.	индивидуальное задание
15.	Идентификация. Фиксированные пароли. Парольные фразы.	индивидуальное задание
16.	Цифровые подписи. Одноразовые цифровые подписи.	индивидуальное задание

2.3.4 Примерная тематика курсовых работ (проектов)

Курсовые работы - не предусмотрены

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	Базовые понятия и история развития информационной безопасности.	Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, И. П. Слинькова, В. В. Гафнер, П. А. Кисляков ; М-во образования и науки Рос. Федерации, ФГБОУ ВПО "Новосибирский гос. пед. ун-т", ФГБОУ ВПО "Моск. пед. гос. ун-т". - Москва ; Новосибирск : [АРТА], 2012 Стандарты оформления исходного кода программ и современные интегрированные среды разработки программного обеспечения: учеб.-метод.пособие. Ю.В. Кольцов [и др.] – Краснодар: Кубанский гос.ун-т, 2017

2	Конечные поля. Многочлены над конечным полем. Последовательности над конечным полем.	Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, И. П. Слинькова, В. В. Гафнер, П. А. Кисляков ; М-во образования и науки Рос. Федерации, ФГБОУ ВПО "Новосибирский гос. пед. ун-т", ФГБОУ ВПО "Моск. пед. гос. ун-т". - Москва; Новосибирск: [АРТА], 2012 Стандарты оформления исходного кода программ и современные интегрированные среды разработки программного обеспечения: учеб. - метод. Пособие. Ю.В. Кольцов [и др.] – Краснодар: Кубанский гос.ун-т, 2017
3	Шифры замены. Шифры перестановки. Шифры гаммирования.	Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, И. П. Слинькова, В. В. Гафнер, П. А. Кисляков ; М-во образования и науки Рос. Федерации, ФГБОУ ВПО "Новосибирский гос. пед. ун-т", ФГБОУ ВПО "Моск. пед. гос. ун-т". - Москва ; Новосибирск : [АРТА], 2012 Стандарты оформления исходного кода программ и современные интегрированные среды разработки программного обеспечения: учеб.-метод.пособие. Ю.В. Кольцов [и др.] – Краснодар: Кубанский гос.ун-т, 2017
4	Блочные системы шифрования.	Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, И. П. Слинькова, В. В. Гафнер, П. А. Кисляков ; М-во образования и науки Рос. Федерации, ФГБОУ ВПО "Новосибирский гос. пед. ун-т", ФГБОУ ВПО "Моск. пед. гос. ун-т". - Москва; Новосибирск : [АРТА], 2012 Стандарты оформления исходного кода программ и современные интегрированные среды разработки программного обеспечения: учеб.-метод.пособие. Ю.В. Кольцов [и др.] – Краснодар: Кубанский гос.ун-т, 2017
№	**Вид СРС**	**Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы**
5	Поточные истемы шифрования.	Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, И. П. Слинькова, В. В. Гафнер, П. А. Кисляков ; М-во образования и науки Рос. Федерации, ФГБОУ ВПО "Новосибирский гос. пед. ун-т", ФГБОУ ВПО "Моск. пед. гос. ун-т". - Москва; Новосибирск: [АРТА], 2012 Стандарты оформления исходного кода программ и современные интегрированные среды разработки программного обеспечения: учеб.-метод.пособие. Ю.В. Кольцов [и др.] – Краснодар: Кубанский гос.ун-т, 2017

6	Идентификация. Цифровые подписи.	Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, И. П. Слинькова, В. В. Гафнер, П. А. Кисляков ; М-во образования и науки Рос. Федерации, ФГБОУ ВПО "Новосибирский гос. пед. ун-т", ФГБОУ ВПО "Моск. пед. гос. ун-т". - Москва; Новосибирск : [АРТА], 2012 Стандарты оформления исходного кода программ и современные интегрированные среды разработки программного обеспечения: учеб.-метод.пособие. Ю.В. Кольцов [и др.] – Краснодар: Кубанский гос.ун-т, 2017

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.

В соответствии с требованиями ФГОС в программа дисциплины предусматривает использование в учебном процессе следующих образовательные технологии: чтение лекций с использованием мультимедийных технологий; метод малых групп, разбор практических задач и кейсов.

При обучении используются следующие образовательные технологии:

- Технология коммуникативного обучения – направлена на формирование коммуникативной компетентности студентов, которая является базовой, необходимой для адаптации к современным условиям межкультурной коммуникации.

- Технология разноуровневого (дифференцированного) обучения – предполагает осуществление познавательной деятельности студентов с учётом их индивидуальных способностей, возможностей и интересов, поощряя их реализовывать свой творческий потенциал. Создание и использование диагностических тестов является неотъемлемой частью данной технологии.

- Технология модульного обучения – предусматривает деление содержания дисциплины на достаточно автономные разделы (модули), интегрированные в общий курс.

- Информационно-коммуникационные технологии (ИКТ) - расширяют рамки образовательного процесса, повышая его практическую направленность, способствуют

интенсификации самостоятельной работы учащихся и повышению познавательной активности. В рамках ИКТ выделяются 2 вида технологий:

− Технология использования компьютерных программ – позволяет эффективно дополнить процесс обучения языку на всех уровнях.

− Интернет-технологии – предоставляют широкие возможности для поиска информации, разработки научных проектов, ведения научных исследований.

− Технология индивидуализации обучения – помогает реализовывать личностно ориентированный подход, учитывая индивидуальные особенности и потребности учащихся.

− Проектная технология – ориентирована на моделирование социального взаимодействия учащихся с целью решения задачи, которая определяется в рамках профессиональной подготовки, выделяя ту или иную предметную область.

− Технология обучения в сотрудничестве – реализует идею взаимного обучения, осуществляя как индивидуальную, так и коллективную ответственность за решение учебных задач.

− Игровая технология – позволяет развивать навыки рассмотрения ряда возможных способов решения проблем, активизируя мышление студентов и раскрывая личностный потенциал каждого учащегося.

− Технология развития критического мышления – способствует формированию разносторонней личности, способной критически относиться к информации, умению отбирать информацию для решения поставленной задачи.

Комплексное использование в учебном процессе всех вышеназванных технологий стимулируют личностную, интеллектуальную активность, развивают познавательные процессы, способствуют формированию компетенций, которыми должен обладать будущий специалист.

Основные виды интерактивных образовательных технологий включают в себя: − работа в малых группах (команде) - совместная деятельность студентов в группе под руководством лидера, направленная на решение общей задачи путём творческого сложения результатов индивидуальной работы членов команды с делением полномочий и ответственности;

− проектная технология - индивидуальная или коллективная деятельность по отбору, распределению и систематизации материала по определенной теме, в результате которой составляется проект;

− анализ конкретных ситуаций - анализ реальных проблемных ситуаций, имевших место в соответствующей области профессиональной деятельности, и поиск вариантов лучших решений;

− развитие критического мышления – образовательная деятельность, направленная на развитие у студентов разумного, рефлексивного мышления, способного выдвинуть новые идеи и увидеть новые возможности.

Подход разбора конкретных задач и ситуаций широко используется как преподавателем, так и студентами во время лекций, лабораторных занятий и анализа

результатов самостоятельной работы. Это обусловлено тем, что при исследовании и решении каждой конкретной задачи имеется, как правило, несколько методов, а это требует разбора и оценки целой совокупности конкретных ситуаций.

Темы, задания и вопросы для самостоятельной работы призваны сформировать навыки поиска информации, умения самостоятельно расширять и углублять знания, полученные в ходе лекционных и практических занятий.

Подход разбора конкретных ситуаций широко используется как преподавателем, так и студентами при проведении анализа результатов самостоятельной работы.

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

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.

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

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

4.1Фонд оценочных средств для проведения текущего контроля.

Индивидуальные задачи (выполняются студентами самостоятельно и предоставляются в письменном виде).

1. Алгоритм DES. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
2. Алгоритм A5. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
3. Алгоритм Feal. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
4. Алгоритм Crypto1. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

5. Алгоритм IDEA. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма Dragon. Реализовать в виде программного приложения с оконным интерфейсом.
6. Алгоритм ГОСТ 94. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
7. Алгоритм Mickey. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма Safer64. Реализовать в виде программного приложения с оконным интерфейсом.
8. Алгоритм Mosqito. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма RC5-64. Реализовать в виде программного приложения с оконным интерфейсом.
9. Алгоритм Rabbit. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
10. Алгоритм Loki 91. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма RC4. Реализовать в виде программного приложения с оконным интерфейсом.
11. Алгоритм CAST256. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
12. Алгоритм SEAL. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
13. Алгоритм AES. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
14. Алгоритм GMR. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
15. Алгоритм Wake. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
16. Алгоритм Trivium. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
17. Алгоритм Skipjack. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

18. Алгоритм Vest. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

19. Алгоритм Frog. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

20. Алгоритм VMPC. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

21. Алгоритм Serpent. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

22. Алгоритм Oryx. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

23. Алгоритм TEA. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

24. Алгоритм Salsa20. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

25. Алгоритм Mars. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

26. Алгоритм Mugi. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

27. Алгоритм Blowfish. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

28. Алгоритм Pike. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

29. Алгоритм ГОСТ 2012. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

30. Алгоритм DSA. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

4.2 Фонд оценочных средств для проведения промежуточной аттестации.

Вопросы для промежуточной аттестации по итогам освоения дисциплины:

1. Группа. Подгруппа.
2. Группа постановок.
3. Кольцо. Идеалы. Классы вычетов.
4. Кольца полиномов.
5. Конечные поля.
6. Кольцо вычетов.
7. Алгоритмы умножения, обращения, вычисления НОД.
8. Извлечение корней в конечном поле.
9. Вычисление символа Якоби. Проверка на простоту.
10. Основные понятия и определения криптографической защиты информации.
11. Шифрование.
12. Аутентификация.
13. Система RSA. Детерминированные методы разложения.
14. Система RSA. Вероятностные методы разложения.
15. Дискретное логарифмирование в конечном поле. Задача Диффи-Хеллмана.
16. Шифрование с открытым ключом для группы вычислимого порядка.
17. Шифрование с открытым ключом для группы трудно вычислимого порядка.
18. Цифровая подпись на группе трудно вычислимого порядка.
19. Цифровая подпись на группе вычислимого порядка.
20. Схемы предъявления битов. Криптографические протоколы доказательства с нулевым разглашением.
21. Криптографические протоколы передачи информации со стиранием. Криптографический протокол разделения секрета.
22. Криптографические протоколы управления ключами. Временная метка.
23. Основные понятия классической криптографии. Шифры замены и перестановки. Блочные шифры.
24. Режимы шифрования.
25. Шифр DES.
26. Шифр FEAL.
27. Шифр IDEA.
28. Шифр ГОСТ 28147-89.
29. Шифр RC5.
30. Шифр Blowfish.
31. Шифр SAFER.
32. Шифр AES.
33. Шифр MD5.
34. Шифр ГОСТ Р 34.11-94.

35. Хэш-функция. Хэширование.

Критерий оценивания:

Оценка		
Удовлетворительно	**Хорошо**	**Отлично**
• если студент указал направление решения задачи и получил «удовлетворительно» по двум вопросам • если студент верно решил задачу; получил «хорошо» или «отлично» по ответу хотя бы на один вопрос	• если студент в целом верно решил задачу и получил «хорошо» по двум вопросам • если студент в целом верно решил задачу и получил «удовлетворительно» по одному вопросу и «отлично» хотя бы на один вопрос	• если студент верно решил задачу и получил «хорошо» хотя бы по одному вопросу и «отлично» по другому

Оценка «неудовлетворительно» выставляется при невозможности поставить оценку «Удовлетворительно», «Хорошо», «Отлично»

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.

5.1 Основная литература:

1. Прохорова, О.В. Информационная безопасность и защита информации: учебник /

О.В. Прохорова; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно строительный университет». - Самара: Самарский государственный архитектурно строительный университет, 2014. - http://biblioclub.ru/index.php?page=book&id=438331.

2. Лапонина, О.Р. Криптографические основы безопасности / О.Р. Лапонина. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016.
3. Петренко, В.И. Теоретические основы защиты информации: учебное пособие / В.И. Петренко; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «СевероКавказский федеральный университет». - Ставрополь: СКФУ, 2015. – https://biblioclub.ru/index.php?page=book_red&id=458204&sr=1
4. Фороузан, Б.А. Математика криптографии и теория шифрования / Б.А. Фороузан. -

2-е изд., испр. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. - https://biblioclub.ru/index.php?page=book_red&id=428998&sr=1

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечных системах «Лань» и «Юрайт».

5.2 Дополнительная литература:

1. Басалова, Г.В. Основы криптографии: курс лекций / Г.В. Басалова; Национальный Открытый Университет "ИНТУИТ". - Москва: Интернет-Университет Информационных Технологий, 2011. - 253 с.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=233689 2. Сергеева, Ю.С.

Защита информации. Конспект лекций [Электронный ресурс]: учеб. пособие — Электрон. дан. — Москва: А-Приор, 2011. – https://biblioclub.ru/index.php?page=book_red&id=72670&sr=1 3. Голиков, А.М.

Защита информации в инфокоммуникационных системах и сетях: учебное пособие / А.М. Голиков; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск: Томский государственный университет систем управления и радиоэлектроники, 2015. – https://biblioclub.ru/index.php?page=book_red&id=480637&sr=1

4. Долозов, Н.Л. Программные средства защиты информации: конспект лекций / Н.Л. Долозов, Т.А. Гультяева ; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. - Новосибирск: НГТУ, 2015. – https://biblioclub.ru/index.php?page=book_red&id=438307&sr=1
5. Бабенко, Л.И. Параллельные алгоритмы для решения задач защиты информации / Л.И. Бабенко, Е.А. Ищукова, И.Д. Сидоров. - Москва: Издательство Горячая линия Телеком, 2014. - https://e.lanbook.com/reader/book/63228/#1.

5.3. Периодические издания:

1. Вычислительные методы и программирование
2. Математическое моделирование
3. Прикладная информатика
4. Программирование

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

1. Назначение и структура алгоритмов шифрования— URL:http://www.ixbt.com/soft/alg-encryption.shtml
2. Криптографические алгоритмы, применяемые для обеспечения информационной безопасности при взаимодействии в ИНТЕРНЕТURL:http://www.bnti.ru/showart.asp?aid=797&lvl=04.03.07.

7. Методические указания для обучающихся по освоению дисциплины.

По дисциплине предусмотрено проведение практических занятий, на которых дается прикладной систематизированный материал. В ходе занятий разбираются алгоритмы и структуры представления графов, а также приводятся примеры разработки программных приложений. После практического занятия рекомендуется выполнить упражнения, приводимые в аудитории для самостоятельной работы.

При самостоятельной работе студентов необходимо изучить литературу, приведенную в перечнях выше, для осмысления вводимых понятий, анализа предложенных подходов и методов разработки программ. Разрабатывая решение новой задачи, студент должен уметь выбрать эффективные и надежные структуры данных для представления информации, подобрать соответствующие алгоритмы для их обработки, учесть специфику языка программирования, на котором будет выполнена реализация. Студент должен уметь

выполнять тестирование и отладку алгоритмов решения задач с целью обнаружения и устранения в них ошибок.

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.

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

Перечень информационных технологий.

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

Перечень необходимого программного обеспечения.

– КомпиляторязыкаC++(«MicrosoftVisualStudio 12»).
– Программы для демонстрации и создания презентаций («MicrosoftPowerPoint»). – Программы, поддерживающие OLE сервера(«MicrosoftWord», «MicrosoftExcel»).

Перечень информационных справочных систем:

1. Справочно-правовая система «Консультант Плюс» (http://www.consultant.ru)
2. Электронная библиотечная система eLIBRARY.RU (http://www.elibrary.ru)/

Материально-техническая база, необходимая для осуществления образовательногопроцесса по дисциплине.

№	Вид работ	Материально-техническое обеспечение дисциплины и оснащенность
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 MS Windows, MicrosoftVisualStudio 12, MicrosoftPowerPoint, MicrosoftWord, MicrosoftExcel

3.	Текущий контроль, промежуточная аттестация	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, компьютерами, программным обеспечением MS Windows, MicrosoftVisualStudio 12, MicrosoftPowerPoint, MicrosoftWord, MicrosoftExcel
4.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет»,программой экранного увеличения и обеспеченный доступом в электронную информационнообразовательную среду университета.