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

«29» мая 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) Б1.В.ДВ.03.02 МАТЕМАТИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки/специальность *01.03.02 Прикладная математика и информатика*

Направленность (профиль) / специализация *Программирование и информационные технологии*

Форма обучения *очная*

Квалификация *бакалавр*

Краснодар 2020

Рабочая программа дисциплины «Математические методы защиты информации» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки / специальности 01.03.02 Прикладная математика и информатика

Программу составил(и):

В.В. Подколзин, доцент, канд. физ.-мат. наук _____
И.О. Фамилия, должность, ученая степень, ученое звание подпись

О.В. Гаркуша, доцент, канд. физ.-мат. наук, доцент _____
И.О. Фамилия, должность, ученая степень, ученое звание подпись

Рабочая программа дисциплины «Математические методы защиты информации» утверждена на заседании кафедры информационных технологий протокол № 18 от «06» мая 2020 г.

И. о. зав. кафедрой (разработчика) О.В. Гаркуша _____
фамилия, инициалы подпись

Рабочая программа обсуждена на заседании кафедры утверждена на заседании кафедры информационных технологий протокол № 18 от «06» мая 2020 г.

И. о. зав. кафедрой (выпускающей) О.В. Гаркуша _____
фамилия, инициалы подпись

Утверждена на заседании учебно-методической комиссии факультета компьютерных технологий и прикладной математики протокол № 2 от «22» мая 2020г.

Председатель УМК факультета Коваленко А.В _____
фамилия, инициалы подпись

Рецензенты:

Рубцов Сергей Евгеньевич, кандидат физико-математических наук, доцент кафедры математического моделирования ФГБГОУ «КубГУ»

Бегларян Маргарита Евгеньевна, кандидат физико-математических наук, доцент, заведующий кафедрой СГЕНД СКФ ФГБОУ ВО «Российский государственный университет правосудия»

1 Цели и задачи изучения дисциплины.

1.1 Цель освоения дисциплины.

Курс посвящен изучению современных концепций информационной безопасности и их применения в обеспечении защиты информации и безопасного использования программных средств в вычислительных системах. Цель курса – научить студента методам информационной безопасности и их использовании в области защиты информации. Задачей курса является изложение теории информационной безопасности и практики применения алгоритмов криптозащиты.

Воспитательной целью дисциплины является формирование у студентов научного, творческого подхода к освоению технологий, методов и средств производства и защиты программного обеспечения. Дать студентам математические основы защиты информации.

Отбор материала основывается на необходимости ознакомить студентов со следующей современной научной информацией:

методы защиты информации;

области применения защиты информации;

о технологиях анализа шифров.

Содержательное наполнение дисциплины обусловлено общими задачами в подготовке бакалавра.

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.

Студент в рамках курса должен знать области применения задач информационной безопасности; методы защиты информации; области применения различных методов информационной безопасности; этапы, методы и инструментальные средства информационной безопасности. принципы построения и функционирования систем информационной безопасности; классификацию шифров; основы организации идентификации и цифровой подписи; принципы построения и применения паролей; уметь проводить анализ и определять оптимальный метод защиты информации; формировать требования к предметно-ориентированной системе информационной безопасности и определять возможные пути их выполнения; формулировать и решать задачи организации процесса цифровой подписи; формулировать и решать задачи организации процесса идентификации; реализовать на языке программирования заданный метод защиты информации; решать задачи анализа шифра.

В качестве основной формы итогового контроля по рассматриваемой дисциплине предусмотрен зачет.

1.2 Задачи дисциплины.

Основные задачи курса на основе системного подхода:

иметь базовые знания по основам теории защиты информации;

уметь на практике реализовывать различные методы надёжной и быстрой защиты информации;

уметь при решении конкретной задачи профессионально грамотно сформулировать задачу передачи электронных данных;

иметь базовые знания о методах передачи и защиты конфиденциальной информации;

расширение практической базы для изучения других учебных дисциплин, таких, как "Технология разработки программного обеспечения ", "Архитектура вычислительных и компьютерных систем" и др.

Содержательное наполнение дисциплины обусловлено общими задачами в подготовке бакалавра.

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

1.3 Место дисциплины в структуре образовательной программы.

Курс «Математические методы защиты информации» входит в вариативную часть Блока 1 «Дисциплины (модули)» дисциплин, формирующих знания и навыки в области разработки современного программного обеспечения. Курс опирается на знания курсов «Математическая логика и дискретная математика», «Языки программирования и методы трансляции», «Основы сетевых технологий». Курс расширяет знания студентов в области создания программных систем, защиты данных и знаний.

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

В результате освоения дисциплины студент должен:

Знать:

1. Математические основы теории передачи и защиты информации
2. Проблемы передачи, обнаружения и исправления внутриканальных ошибок;
3. Способы кодирования информации;
4. Знать источники угроз безопасности информации и методы оценки уязвимости;
5. Методы создания, организации и обеспечения функционирования систем;
6. Основные границы относительно мощности кодов.

Уметь:

7. Анализировать политику безопасности;
8. Профессионально грамотно сформулировать конфиденциальную задачу;
9. На практике осуществлять концепцию обеспечения информационной безопасности.

Владеть:

10. Владение основными методами, способами и средствами получения, хранения, переработки информации, иметь навыки работы с компьютером как средством управления информацией;
11. Основными методами и средствами безопасной защиты информации;
12. Современными технологиями защиты информации в целом.

Изучение данной учебной дисциплины направлено на формирование у обучающихся компетенций

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ПК-1	способностью собирать, обрабатывать и интерпретировать данные современных научных исследований, необходимые для формирования выводов по соответствующим научным	4, 5, 6	7	11, 12

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
		исследованиям			
2.	ОПК-4	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	1, 2, 3	8, 9	10

2. Структура и содержание дисциплины.

2.1 Распределение трудоёмкости дисциплины по видам работ.

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

Вид учебной работы		**Всего часов**	**Семестры (часы)**			
			7	**___**		
Контактная работа, в том числе:						
Аудиторные занятия (всего):						
Занятия лекционного типа		-	-	-	-	-
Лабораторные занятия		54	54	-	-	-
Занятия семинарского типа (семинары, практические занятия)				-	-	-
Иная контактная работа:						
Контроль самостоятельной работы (КСР)		6	6			
Промежуточная аттестация (ИКР)		0,2	0,2			
Самостоятельная работа, в том числе:						
Проработка учебного (теоретического) материала		20	20	-	-	-
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		25	25	-	-	-
Подготовка к текущему контролю		2,8	2,8	-	-	-
Контроль:						
Подготовка к экзамену						
Общая трудоемкость	**час.**	**108**	**108**	**-**	**-**	**-**
	в том числе контактная работа	**60,2**	**60,2**			
	зач. ед	**3**	**3**			

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы дисциплины, изучаемые в6семестре (очная форма).
Вид промежуточной аттестации: ЗАЧЕТ.

№	**Наименование разделов**	**Количество часов**

		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	Основы теории защиты информации	14			8	6
2	Линейное и нелинейное кодирование. Корректирующие свойства кодов	22			12	10
3	Конечные поля	30			16	14
4	Обнаружение и исправление ошибок	25			16	9
5	Обзор изученного материала и прием зачета	11			2	8,7
	Контроль самостоятельной работы (КСР)	6				
	Промежуточная аттестация (ИКР)	0,2				
	Итого по дисциплине:	108			54	47,8

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

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа.

Не предусмотрены

2.3.2 Занятия семинарского типа.

Не предусмотрены

2.3.3 Лабораторные занятия.

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1.	Теория информации и её энтропия	Различные подходы. Сравнение неопределённостей. Примеры	собеседование
2.	Количественная мера по Хартли, по Шеннону и А.Н. Колмогорову	Мера неопределённости информации. Количество информации и его свойства	собеседование, индивидуальное задание
3.	Алфавит дискретных логических устройств	Простые конечные поля и их свойства. Конечное поле GF(q) и его свойства	собеседование, индивидуальное задание
4.	Теория кодирования	Примеры кодов. Коды Хэмминга. Совершенность кодов Хэмминга	собеседование, индивидуальное задание
5.	Циклические коды	Описание циклических кодов. AN-циклические коды и их свойства	собеседование, индивидуальное задание

№	Наименование раздела	Содержание раздела	Форма текущего контроля
6.	Коды БЧХ, исправляющие две ошибки	Обобщение линейных кодов. Обнаружение и исправление двух симметричных ошибок	собеседование, индивидуальное задание
7.	Матрицы Адамара. Нелинейные коды.	Существование матриц Адамара. Коды Адамара	собеседование, индивидуальное задание
8.	Границы мощности кодов	Граница сферической упаковки. Граница Р.Р. Варшамова и др.	собеседование, 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	Теория информации и её энтропия	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.	Количественная мера по Хартли, по Шеннону и А.Н. Колмогорову	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.	Алфавит дискретных логических устройств	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

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
		современные интегрированные среды разработки программного обеспечения: учеб.-метод.пособие. Ю.В. Кольцов [и др.] – Краснодар: Кубанский гос.ун-т, 2017
4.	Теория кодирования	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
5.	Циклические коды	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.	Коды БЧХ, исправляющие две ошибки	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
7.	Матрицы Адамара. Нелинейные коды.	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
8.	Границы мощности кодов	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

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

Семестр	Вид занятия	Используемые интерактивные образовательные технологии	количество интерактивных часов
7	ЛР	Занятия в режимах взаимодействия «преподаватель – студент» и «студент – студент»	10
Итого			10

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.

Учебная деятельность проходит в соответствии с графиком учебного процесса. Процесс самостоятельной работы контролируется во время аудиторных занятий и индивидуальных консультаций. Самостоятельная работа студентов проводится в форме изучения отдельных теоретических вопросов по предлагаемой литературе.

Фонд оценочных средств дисциплины состоит из средств текущего контроля (опрос по результатам индивидуальных заданий, тестирование) и итоговой аттестации: зачета.

Перечень заданий текущего контроля по темам:

Перечень компетенций, проверяемых оценочным средством:

ПК-1 способностью собирать, обрабатывать и интерпретировать данные современных научных исследований, необходимые для формирования выводов по соответствующим научным исследованиям

ОПК-4 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

1. Коды Варшамова. Обнаружение и исправление несимметричных одиночных ошибок. Примеры
2. Квадратично-вычетные коды. Граница квадратичного корня
3. Корректирующие возможности арифметических **AN**-кодов
4. Методы комбинирования кодов.
5. Доказать, что каждый ненулевой элемент поля GF(P) имеет обратный элемент
6. Определить число примитивных элементов поля $GF(P)$
7. Доказать, что для произвольных двух элементов $a, b \in GF(P)$ имеет место равенство $(a + b)^P = a^P + b^P$
8. Доказать, что $(P – 1)! = – 1$
9. Доказать, что если $f (x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n, a_n \in GF(P)$, то $f (x^P) = (f (x))^P$
10. Доказать, что корнями уравнения $x^P - x = 0$ являются все элементы поля $GF(P)$
11. Найти число $N_P(a x + b)$ всех линейных функций $y = a x + b$ в $GF(P)$
12. Найти число $N_P((a x + b) / (c x + d))$ всех дробно - линейных функций $y = (a x + b) / (c x + d)$ в $GF(P)$
13. Определить число $N_P (a d - b c = k)$ в $GF(P)$, где $k \in GF(P)$
14. Найти число решений $N_P (x_1 + x_2 + \ldots + x_n = k)$ уравнения $x_1 + x_2 + \ldots + x_n = k$ в $GF(P)$, где $k \in GF(P)$

15. Доказать, что $x^P - x = F_1(x) F_P(x)$, где $F_1(x)$ и $F_P(x)$ произведения всех простых над GF(P) полиномов степеней 1 и P соответственно
16. Определить число $I_P(n)$ простых над GF(P) полиномов степени n. Доказать, что $I_P(n) \geq 1$
17. Разработать алгоритм построения простого над GF(P) полиномов заданной степени в явном виде

Зачетно-экзаменационные материалы для промежуточной аттестации (зачет)

Список задач и вопросов для подготовки к промежуточной аттестации

Перечень компетенций, проверяемых оценочным средством:

ПК-1 способностью собирать, обрабатывать и интерпретировать данные современных научных исследований, необходимые для формирования выводов по соответствующим научным исследованиям

ОПК-4 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Список вопросов для подготовки к зачету

1. Информация и неопределённость. Количественная мера неопределённости. Подходы Р. Хартли, К. Шеннона и А.Н. Колмогорова
2. Алфавит дискретных устройств. Конечные поля
3. Простое поле Галуа GF(P). Составное поле Галуа $GF(P^n)$
4. Математические методы защиты информации от помех в каналах связи
5. Кодирование информации. Основные понятия. Примеры
6. Линейные коды. Способы их задания
7. Свойства линейного кода. Коды Хэмминга
8. Граница Хэмминга. Граница Варшамова-Гильберта
9. Коды Варшамова. Обнаружение и исправление несимметричных одиночных ошибок
10. Циклические коды и их описание
11. Коды БЧХ, исправляющие две ошибки
12. Нелинейные коды. Коды Адамара
13. Совершенные коды. Двоичный код Голея
14. Квадратично-вычетные коды. Граница квадратичного корня
15. Арифметические AN-коды и их свойства
16. Корректирующие возможности арифметических AN-кодов
17. Коды Рида-Соломона и их корректирующие возможности
18. Коды Рида-Маллера и их корректирующие возможности
19. Методы комбинирования кодов
20. Повышение надёжности цифровых устройств с помощью корректирующих кодов
21. Границы мощности кодов
22. Информация и неопределённость
23. Количественная мера неопределённости
24. Условная неопределённость. Количество информации
25. Передача информации
26. Пропускная способность канала связи. Теоремы Шеннона
27. Сжатие информации. Метод Шеннона-Фано

Примерные задачи для подготовки к зачету

1. Доказать, что два поля Галуа с одним и тем же числом элементов изоморфны
2. Доказать, что над каждым полем GF(q) существует примитивный полином любой положительной степени.
3. Пусть x = x 1x 2 . . .x n , y = y 1 y 2 . . . y n∈GF(2 n). Установить связь между расстояниями Хэмминга d X (x , y) и Евклида d E (x , y)
4. Доказать, что для расстояния Хэмминга выполняется неравенство треугольника d (x , y) ≤ d (x , z) + d (z , y)
5. Доказать, что H x' т = 0 тогда и только тогда, когда шумовое слово равно нулю
6. Для фиксированной длины n определить наименьшее число избыточных символов
7. Доказать, что если H = (A | E r) , то G = (E к| - A кт)
8. Доказать, что d (x , y) = d (x + z , y + z) = W (x + y)
9. Разработать алгоритм декодирования линейных блочных кодов
10. Доказать, что код с кодовым расстоянием d может исправлять [(d - 1)/2] ошибок, причём если d чётное, то он может одновременно исправлять (d - 1)/2 ошибок и обнаруживать d/2 ошибок
11. Доказать, что если H - проверочная матрица линейного кода длины n , то код имеет минимальное расстояние d тогда и только тогда, когда любые d - 1 столбцов матрицы H линейно независимы, но найдутся d линейно зависимых столбцов
12. Доказать, что если i, j,. . ., k - номера ошибочных позиций принятого слова x' некоторого линейного кода с проверочной матрицей H, то S = Hx '= Hi+ Hj + . . . + Hk , где Hi - i- й столбец матрицы H
13. Доказать, что кодовое расстояние кодов Хэмминга равно 3
14. Доказать, что кодовое расстояние расширенных кодов Хэмминга равно 4
15. Построить проверочную матрицу [13 , 10 , 3] - кода Хэмминга над полем GF(3)
16. Доказать, что если C - двоичный линейный код и слово a∉ C, то CU(a+C) также является двоичным линейным кодом
17. 1
18. Доказать, что если C является [n , k , d]- кодом над полем GF(P), то множество всех слов GFn(P) можно разбить на непересекающиеся смежные классы: GFn(P) = C U (a 1 + C) U (a 2 + C) U . . . U (a t + C) , где t = P n - k -1
19. Доказать, что если C – [n , k , d]- код , то d ≤ n - k + 1 (Граница Синглтона)
20. Определить веса всех кодовых слов (спектр весов) кода H r.

Компонентом промежуточного контроля по дисциплине «Математические методы защиты информации» являются решение задачи из списка задач к промежуточной аттестации и ответа на два теоретических вопроса. Максимальное количество баллов, которые студент может получить за ответ вопрос, составляет 6 баллов. Максимальное количество баллов, которые студент может получить за правильное решение задачи составляет 3 балла.

Количество баллов, которое студенты могут получить за выполнение заданий определяется согласно таблицы:

Описание	**Баллы**
Вопрос	
Студент владеет теоретическими знаниями по данному вопросу, что подтверждается его ответами на дополнительные вопросы; студент умеет правильно объяснять теоретический материал, иллюстрируя его примерами;	5-6
Студент владеет теоретическими знаниями по данному вопросу, при ответе студент допускает незначительные ошибки; студент умеет правильно объяснять теоретический материал;	3-4
Теоретический материал не усвоен или усвоен частично, студент не может предоставить четкий ответ на поставленный вопрос; студент затрудняется привести примеры, поясняющие ответы на вопросы;	0-2
Задача	
Задача решена правильно, студент может пояснить ход решения	2
Задача решена неправильно, однако решение задачи показывает, что студент понимает материал, студент может пояснить ход решения,	1

Задача решена неправильно, решение задачи показывает, что студент не понимает материал	0

Критерии оценки:

Оценка	
Незачет	**Зачтено**
• студент получил 0 баллов за задачу и менее 5 баллов по каждому из двух вопросов	• студент получил не менее 1 балла за задачу и не менее 3 баллов за один из двух вопросов; • студент получил не менее 4 балла за задачу; • студент получил не менее 1 балла за задачу и не менее 5 баллов за один из двух вопросов • студент получил не менее 2 баллов за задачу и не менее 5 баллов за один из двух вопросов; студент получил не менее не менее 10 баллов за два вопроса студент получил 3 балла за задачу и не менее 11 баллов за два вопроса, ответил на дополнительные вопросы

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. Баранова, Е.К. Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие / Е. К. Баранова, А. В. Бабаш . - 3-е изд., перераб. и доп. - М. : РИОР : ИНФРА-М, 2017. - 322 с. - http://znanium.com/catalog.php?bookinfo=763644

2. Прохорова, О.В. Информационная безопасность и защита информации [Электронный ресурс] : учебник / О.В. Прохорова. - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. - http://biblioclub.ru/index.php?page=book&id=438331.
3. Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия [Текст] : учебное пособие для студентов вузов / О. Р. Лапонина ; [под ред. В. А. Сухомлина]. - 2-е изд., испр. - М. : Интернет-Университет Информационных Технологий : БИНОМ. Лаборатория знаний , 2007. - 531 с

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. Бабаш, А. В. Криптографические методы защиты информации [Текст] : учебник для студенто вузов, обучающихся по направлению "Прикладная информатика" / А. В. Бабаш, Е. К. Баранова. - Москва : КНОРУС, 2016. - 189 с
2. Корт, С. С. Теоретические основы защиты информации [Текст] : учебное пособие для студентов вузов / С. С. Корт. - М. : Гелиос АРВ , 2004. - 233 с
3. Бабенко, Л.К. Параллельные алгоритмы для решения задач защиты информации [Электронный ресурс] : учебное пособие / Л.К. Бабенко, Е.А. Ищукова, И.Д. Сидоров. — Электрон. дан. — Москва : Горячая линия-Телеком, 2014. — 304 с. — Режим доступа: https://e.lanbook.com/book/63228
4. В.О. Осипян, К.В. Осипян Математические основы теории и практики защиты информации [Текст] : учебное пособие / В. О. Осипян, К. В. Осипян ; М-во образования Рос. Федерации, Кубанский гос. ун-т. - Краснодар : [КубГУ], 2003.
5. Осипян В.О. Разработка методов построения систем передачи и защиты информации [Текст] / В. О. Осипян ; М-во образования и науки Рос. Федерации, Кубанский гос. ун-т. - Краснодар : [КубГУ], 2004. - 179 с.

5.3. Периодические издания:

1. Вычислительные методы и программирование
2. Вестник информационной безопасности
3. Защита персональных данных
4. Вестник кибербезопасности
5. Мир больших данных (big data)
6. Прикладная информатика
7. 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.

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.

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

8.1 Перечень информационных технологий.

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

8.2 Перечень необходимого программного обеспечения.

– Компилятор языка C++
– Программы для безопасной демонстрации и создания презентаций.
– Программы, поддерживающие OLE сервера.

8.3 Перечень информационных справочных систем:

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

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине.

№	Вид работ	Материально-техническое обеспечение дисциплины и оснащенность
1.	Лабораторные занятия	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, компьютерами, проектором, программным обеспечением
2.	Текущий контроль, промежуточная аттестация	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, компьютерами, программным обеспечением
3.	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.