МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный университет имени М.В.Ломоносова»

«Утверждаю»

Декан факультета ВМК МГУ

Ми М.В.Ломоносов

имени М.В. Ломоносова

академик

Е.И. Моисеев

2018 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Дискретные функции в символической динамике»

Уровень высшего образования – подготовка научно-педагогических кадров в аспирантуре

Направление подготовки — 10.06.01 «Информационная безопасность» Направленность (профиль) — «Методы и системы защиты информации, информационная безопасность» (05.13.19)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

1. НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ

Дискретные функции в символической динамике

2. УРОВЕНЬ ВЫСШЕГО ОБРАЗОВАНИЯ

Подготовка научно-педагогических кадров в аспирантуре.

3. НАПРАВЛЕНИЕ ПОДГОТОВКИ, НАПРАВЛЕННОСТЬ (ПРОФИЛЬ) ПОДГОТОВКИ

Направление 10.06.01 «Информационная безопасность». Направленность (профиль) «Методы и системы защиты информации, информационная безопасность» (05.13.19).

4. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к дисциплинам вариативной части образовательной программы и является обязательной для освоения в 3-м семестре обучения.

5. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций образовательной программы:

A	п
Формируемые компетенции	Планируемые результаты обучения
- opp.y obio	in the state of th

Способность разрабатывать и реализовывать алгоритмы организации рабо-	31 (ПК-2) ЗНАТЬ:
ты современных вычислительных комплексов и компьютерных сетей (ПК-2)	современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения У1 (ПК-2) УМЕТЬ: применять современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения В1 (ПК-2) ВЛАДЕТЬ: навыками оптимального выбора современных методов разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения
Владение современными методами построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также методами разработки и реализации алгоритмов их решения на основе фундаментальных знаний в области математики и информатики (ПК-1)	31 (ПК-1) Знать: современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения У1 (ПК-1) Уметь: применять современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения В1 (ПК-1) Владеть: навыками оптимального выбора современных методов построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методов разработки и реализации алгоритмов их решения
Способность формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность (ОПК-1)	31(ОПК-1) ЗНАТЬ научные задачи в области обеспечения информационной безопасности У1(ОПК-1) УМЕТЬ: применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность В1(ОПК-1) ВЛАДЕТЬ: Навыками внедрения полученных результатов в практическую деятельность

Способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности (ОПК-3)	31 (ОПК-3) ЗНАТЬ принципы управления доступом в компьютерных системах, современные методы защиты информации при передаче ее по каналам связи, современные стандарты информационной безопасности У1(ОПК-3) УМЕТЬ: обосновать степень соответствия защищаемых объектов информатизации и информатизационных систем действующим стандартам в области информационной безопасности.
Способность планировать и решать задачи собственного профессионального и личностного развития (УК-5(6))	31(УК-5(6)) ЗНАТЬ: содержание процесса целеполагания профессионального и личностного развития, его особенности и способы реализации при решении профессиональных задач, исходя из этапов карьерного роста и требований рынка труда. У1(УК-5(6)) УМЕТЬ: формулировать цели личностного и профессионального развития и условия их достижения, исходя из тенденций развития области профессиональной деятельности, этапов профессионального роста, индивидуальноличностных особенностей.

Оценочные средства для промежуточной аттестации приведены в Приложении.

6. ОБЪЕМ ДИСЦИПЛИНЫ

Объем дисциплины составляет 3 зачетных единицы, всего 108 часов.

36 часов составляет контактная работа с преподавателем – 34 часа занятий лекционного типа, 0 часов занятий семинарского типа (семинары, научно-практические занятия, лабораторные работы и т.п.), 0 часов индивидуальных консультаций, 0 часа мероприятий текущего контроля успеваемости, 0 часа групповых консультаций, 2 часа мероприятий промежуточной аттестации.

72 часов составляет самостоятельная работа аспиранта.

7. ВХОДНЫЕ ТРЕБОВАНИЯ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Учащиеся должны владеть знаниями по алгебре, дискретной математике и основам кибернетики в объеме, соответствующем основным образовательным программам бакалавриата и магистратуры по укрупненным группам направлений и специальностей 01.00.00 «Математика и механика» и/или 02.00.00 «Компьютерные и информационные науки».

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе обучения не используется программное обеспечение для подготовки слайдов лекций MS PowerPoint.

9. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

В курсе рассматриваются основные понятия символической динамики и развивается атематический аппарат, использующий результаты алгебры, комбинаторики, теории графов и тории автоматов. Анализируются связи основных понятий символической динамики с некоторыми криптографическими примитивами и классами линейных кодов, исправляющими ошибки. Приводятся примеры сведения криптографических и теоретико-кодовых задач к задачам символической динамики.

Наименование и крат-	Всего		В том числе								
кое содержание разделов и тем дисциплины (модуля),	(часы)	Контактная работа (работа во взаимодействии с преподавателем), часы из них					Самостоятельная работа обучаю- щегося, часы из них				
форма промежуточной аттестации по дисциплине (модулю)		Занятия лекционного типа	Занятия семинарско- го типа	Групповые консуль- тации	Индивидуальные консультации	Учебные занятия, направленные на проведение текущего контроля успеваемости (коллоквиумы, практические контрольные занятия и др)*	Всего	Выполнение домашних заданий	Подготовка рефератов и т.п	Всего	

Тема 1. Введение в теорию динамических систем	8	8	-	-	-	8	-	-	-
Метрические пространства. Нормы и метрики. Примеры метрических пространств. Сходимость последовательностей и непрерывность отображений. Открытые и замкнутые множества. Понятие компактности пространства. Критерий компактности множества в компактном пространстве.									
Теорема Больцано . Критерий компактности множества в метрическом пространстве(теорема Гейне-Бореля). Плотность множеств. Теорема Бэра.									
Определение динамической системы Примеры. Инварианты динамических систем. Дзета-функция. Марковские разбиения.									

Тема 2 Сдвиговые пространства (сдвиги) как фазовые пространства в символической динамике.	8	8	-	-	-	-	8	-	-	-
Основные понятия и термины. Полный сдвиг над конечным алфавитом. Примеры. Трансляция и коммутирующие с ней отображения.										
Понятие сдвигового пространства (сдвига). Блоки(слова) — запреты. Примеры. Языки, порождаемые сдвигами. Необходимые и достаточные условия принадлежности слова языку, порожденному сдвигом.										
Сдвиги, порождаемые операциями «расширение» и «расширение» и «расширение с зацеплением». Некоторые свойства и параметры порождаемых сдвиговых пространств										

Тема 3. Скользящие блочные коды.	6	6	-	-	-	-	6	-	-	-
Понятие скользящего блочного кода. Примеры. Простейшие свойства скользящих блочных кодов. Теорема о «гомоморфизме» для скользящего блочного кода. Понятие сопряженности.										
Теретико — кодовые модели скользящих блочных кодов. Сверточные коды, исправляющие ошибки.										
Криптографические модели скользящих блочных кодов. Регистры сдвига с фильтрующими функциями. Фильтрующие и комбинирующие генераторы										

Тема 4. Сдвиговые про- странства конечного типа.	6	6	-	-	-	-	6	-	-	-
Понятие сдвига конечного типа. Примеры. Сдвиги конечного типа с памятью. Теорема о совпадении класса сдвигов конечного типа с классом сдвигов конечного типа с памятью.										
Критерий для сдвигов конечного типа с памятью. Теорема о сопряженности с о сдвигом конечного типа										
Графы и порождаемые ими сдвиги. Примеры. Простейшие свойства сдвигов, порожденных графами. Теоретико-графовое представление сдвигов конечного типа с памятью Софические сдвиги и их простейшие свойства. Понятие энтропии сдвига. Вычисление энтропии.										

Тема 5. Использование методов символической ддинамики для реализации атак на фильтрующие генераторы. Сдвиги, порождаемые линейными полями, и их основные свойства. Фильтрующие функции и их параметры. Использование теоремы о сопряженности для сведения криптографических задачи к задачам символической динамики. Новые криптографические параметры фильтрующих генераторов и их влияние на эффективность решения криптографических задач. Примеры	6	6	-	-	-		6	-	-	-
6. Промежуточная атте- стация – устный экза- мен	74		2 72							
Итого	108				3	6			72	

10. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ УЧАЩИХСЯ

Самостоятельная работа учащихся состоит в изучении лекционного материала, учебно-методической литературы, подготовки к текущему контролю и промежуточной аттестации.

Литература для самостоятельной работы студентов в соответствии с тематическим планом.

- Тема 1 « Введение в теорию динамических систем»
- Тема 2 «Сдвиговые пространства (сдвиги) как фазовые пространства в символической динамике»
- Тема 3 «Скользящие блочные коды»
- Тема 4 «Сдвиговые пространства конечного типа»
- Тема 5 «Использование методов символической ддинамики для реализации атак на фильтрующие генераторы»

11. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ

Основная литература

D.Lind, B.Marcus. An Introduction tj Symbolic Dynamics and Coding. Cambridge University Press 1995, pp. 495.

Ресурсы информационно-телекоммуникационной сети «Интернет»

http://cryptography.ru www.iacr.org

Материально-техническая база

Для преподавания дисциплины требуется класс, оборудованный маркерной или меловой доской.

12. ЯЗЫК ПРЕПОДАВАНИЯ

Русский

13. РАЗРАБОТЧИК ПРОГРАММЫ, ПРЕПОДАВАТЕЛИ

доцент, к.ф.-м.н. Логачев Олег Алексеевич

Приложение

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

«Дискретные функции в символической динамике»

Средства для оценивания планируемых результатов обучения, критерии и показатели оценивания приведены ниже.

РЕЗУЛЬТАТ ОБУЧЕНИЯ по дисциплине (модулю)	КРИТЕРИ (критерии и показат		ОЦЕНОЧНЫЕ СРЕДСТВА						
	1	2	системой оцениван З	4	5				
	Неудовлетворительно	Неудовлетвори-	Удовлетвори-	Хорошо	Отлично				
		тельно тельно							
ЗНАТЬ: научные задачи в области обеспечения информационной безопасности	Отсутствие знаний	Фрагментарные представления о на- учных задачах в об- ласти обеспечения информационной	В целом сформированные, но неполные знания о научных задачах в области обеспе-	Сформированные, но содержащие отдельные пробелы о научных задачах в области	Сформированные систематические знания о научных задачах в области обеспечения инфор-	Устный экзамен			
31(ОПК-1)		безопасности	чения информа- ционной безопас- ности	обеспечения информационной безопасности	мационной безопас- ности				

УМЕТЬ:	Отсутствие умений	Фрагментарные уме-	В целом успеш-	Успешное, но со-	Сформированное	Устный экзамен
применять для задачи		ния применять для	ное, но не систе-	держащее отдель-	умение применять	
в области обеспече-		задачи в области	матическое уме-	ные пробелы уме-	для задачи в области	
ния ИБ решения ме-		обеспечения ИБ ре-	ние применять	ние применять	обеспечения ИБ ре-	
тодологии теорети-		шения методологии	для задачи в об-	для задачи в об-	шения методологии	
ческих и экспери-		теоретических и экс-	ласти обеспече-	ласти обеспече-	теоретических и экс-	
ментальных научных		периментальных на-	ния ИБ решения	ния ИБ решения	периментальных на-	
исследований, вне-		учных исследований,	методологии тео-	методологии тео-	учных исследований,	
дрять полученные		внедрять полученные	ретических и экс-	ретических и экс-	внедрять полученные	
результаты в практи-		результаты в практи-	периментальных	периментальных	результаты в практи-	
ческую деятельность		ческую деятельность	научных исследо-	научных исследо-	ческую деятельность	
У1(ОПК-1)			ваний, внедрять	ваний, внедрять		
			полученные ре-	полученные ре-		
			зультаты в прак-	зультаты в прак-		
			тическую дея-	тическую дея-		
			тельность	тельность		
ВЛАДЕТЬ:	Отсутствие навыков	Фрагментарное вла-	В целом успеш-	Успешное, но со-	Сформированное	устный экзамен
Навыками внедрения		дение навыками вне-	ное, но не полное	держащее отдель-	владение навыками	
полученных резуль-		дрения полученных	владение навыка-	ные пробелы вла-	внедрения получен-	
татов в практическую		результатов в прак-	ми внедрения по-	дение навыками	ных результатов в	
деятельность		тическую деятель-	лученных резуль-	внедрения полу-	практическую дея-	
В1(ОПК-1)		ность	татов в практиче-	ченных результа-	тельность	
			скую деятель-	тов в практиче-		
			ность	скую деятель-		
				ность		

	Отсутствие знаний	Фрагментарные	В целом сформи-	Сформированные,	Сформированные	Устный экзамен
		представления о со-	рованные, но не-	но содержащие	систематические	
DILATI		временных методах	полные знания о	отдельные пробе-	знания о современ-	
ЗНАТЬ:		построения и анализа	современных ме-	лы знания о со-	ных методах по-	
современные методы		математических мо-	тодах построения	временных мето-	строения и анализа	
построения и анализа		делей, возникающих	и анализа матема-	дах построения и	математических мо-	
математических мо-		при решении естест-	тических моде-	анализа матема-	делей, возникающих	
делей, возникающих		веннонаучных задач,	лей, возникающих	тических моде-	при решении естест-	
при решении естест-		а также современных	при решении ес-	лей, возникающих	веннонаучных задач,	
веннонаучных задач,		методах разработки и	тественнонауч-	при решении ес-	а также современных	
а также современные методы разработки и		реализации алгорит-	ных задач, а так-	тественнонауч-	методах разработки и	
реализации алгорит-		мов их решения	же современных	ных задач, а так-	реализации алгорит-	
мов их решения			методах разработ-	же современных	мов их решения	
31 (ПК-1)			ки и реализации	методах разработ-		
31 (IIK-1)			алгоритмов их	ки и реализации		
			решения	алгоритмов их		
				решения		
УМЕТЬ:	Отсутствие умений	Фрагментарные	В целом	Успешное, но	Сформированное	Устный экзамен
применять современ-		умения применять	успешное, но не	содержащее	умение применять	
ные методы построе-		современные методы	систематическое	отдельные	современные методы	
ния и анализа мате-		построения и анализа	умение применять	пробелы умение	построения и анализа	
матических моделей,		математических мо-	современные ме-	применять совре-	математических мо-	
возникающих при		делей, возникающих	тоды построения	менные методы	делей, возникающих	
решении естествен-		при решении естест-	и анализа матема-	построения и ана-	при решении естест-	
нонаучных задач, а		веннонаучных задач,	тических моде-	лиза математиче-	веннонаучных задач,	
также современные		а также современные	лей, возникающих	ских моделей,	а также современные	
методы разработки и		методы разработки и	при решении ес-	возникающих при	методы разработки и	
реализации алгорит-		реализации алгорит-	тественнонауч-	решении естест-	реализации алгорит-	
мов их решения		мов их решения	ных задач, а так-	веннонаучных	мов их решения	
У1 (ПК-1)			же современные	задач, а также со-		
			методы разработ-	временные		
			ки и реализации	методы разработ-		
			алгоритмов их	ки и реализации		
			решения	алгоритмов их		
				решения		

ВЛАДЕТЬ:	Отсутствие навыков	Фрагментарное	В целом	Успешное, но	Сформированное	Устный экзамен
навыками оптималь-		владение навыками	успешное, но не	содержащее	владение навыками	
ного выбора совре-		оптимального выбора	полное владение	отдельные	оптимального выбора	
менных методов по-		современных	навыками опти-	пробелы владение	современных	
строения и анализа		методов построения	мального выбора	навыками опти-	методов построения	
математических мо-		и анализа математи-	современных ме-	мального выбора	и анализа математи-	
делей, возникающих		ческих моделей, воз-	тодов построения	современных ме-	ческих моделей, воз-	
при решении естест-		никающих при реше-	и анализа матема-	тодов построения	никающих при реше-	
веннонаучных задач,		нии естественнона-	тических моде-	и анализа матема-	нии естественнона-	
а также современных		учных задач, а также	лей, возникающих	тических моде-	учных задач, а также	
методов разработки и		современных	при решении ес-	лей, возникающих	современных	
реализации алгорит-		методов разработки и	тественнонауч-	при решении ес-	методов разработки и	
мов их решения		реализации алгорит-	ных задач, а так-	тественнонауч-	реализации алгорит-	
В1 (ПК-1)		мов их решения	же современных	ных задач, а так-	мов их решения	
			методов разра-	же современных		
			ботки и реализа-	методов разра-		
			ции алгоритмов	ботки и реализа-		
			их решения	ции алгоритмов		
				их решения		
	Отсутствие знаний	Фрагментарные	В целом сформи-	Сформированные,	Сформированные	Устный экзамен
		представления о со-	рованные, но не-	но содержащие	систематические	
ЗНАТЬ:		временных методах	полные знания о	отдельные пробе-	знания о современ-	
современные методы		разработки и реали-	современных ме-	лы знания о со-	ных методах разра-	
разработки и реали-		зации алгоритмов	тодах разработки	временных мето-	ботки и реализации	
зации алгоритмов		организации работы	и реализации ал-	дах разработки и	алгоритмов органи-	
организации работы		вычислительных	горитмов органи-	реализации алго-	зации работы вычис-	
вычислительных		комплексов и ком-	зации работы вы-	ритмов организа-	лительных комплек-	
комплексов и ком-		пьютерных сетей по-	числительных	ции работы вы-	сов и компьютерных	
пьютерных сетей по-		следнего поколения	комплексов и	числительных	сетей последнего по-	
следнего поколения			компьютерных	комплексов и	коления	
Код 31 (ПК-2)			сетей последнего	компьютерных		
			поколения	сетей последнего		
				поколения		

УМЕТЬ:	Отсутствие умений	Фрагментарные	В целом	Успешное, но	Сформированное	Устный экзамен
применять современ-		умения применять	успешное, но не	содержащее	умение применять	
ные методы		современные методы	систематическое	отдельные	современные методы	
разработки и		разработки и	умение применять	пробелы умение	разработки и	
реализации		реализации	современные ме-	применять совре-	реализации	
алгоритмов органи-		алгоритмов органи-	тоды разработки и	менные методы	алгоритмов органи-	
зации работы вычис-		зации работы вычис-	реализации алго-	разработки и реа-	зации работы вычис-	
лительных комплек-		лительных комплек-	ритмов организа-	лизации	лительных комплек-	
сов и компьютерных		сов и компьютерных	ции работы вы-	алгоритмов орга-	сов и компьютерных	
сетей последнего		сетей последнего	числительных	низации работы	сетей последнего	
поколения		поколения	комплексов и	вычислительных	поколения	
Код У1 (ПК-2)			компьютерных	комплексов и		
			сетей последнего	компьютерных		
			поколения	сетей последнего		
				поколения		
ВЛАДЕТЬ:	Отсутствие навыков	Фрагментарное	В целом	Успешное, но	Сформированное	Устный экзамен
навыками оптималь-		владение навыками	успешное, но не	содержащее	владение навыками	
ного выбора совре-		оптимального выбора	полное владение	отдельные	оптимального выбора	
менных методов раз-		современных	навыками опти-	пробелы владение	современных	
работки и реализации		методов разработки и	мального выбора	навыками опти-	методов разработки и	
алгоритмов органи-		реализации	современных ме-	мального выбора	реализации	
зации работы вычис-		алгоритмов органи-	тодов разработки	современных ме-	алгоритмов органи-	
лительных комплек-		зации работы вычис-	и реализации ал-	тодов разработки	зации работы вычис-	
сов и компьютерных		лительных комплек-	горитмов органи-	и реализации ал-	лительных комплек-	
сетей последнего		сов и компьютерных	зации работы вы-	горитмов органи-	сов и компьютерных	
поколения		сетей последнего	числительных	зации работы вы-	сетей последнего	
Код В1 (ПК-2)		поколения	комплексов и	числительных	поколения	
			компьютерных	комплексов и		
			сетей последнего	компьютерных		
			поколения	сетей последнего		
				поколения		

ЗНАТЬ:	Отсутствие знаний	Фрагментарные	В целом сформи-	Сформированные,	Сформированные	Устный экзамен
принципы управле-		представления о	рованные, но не-	но содержащие	систематические	
ния доступом в ком-		принципах управле-	полные знания о	отдельные пробе-	знания о принципах	
пьютерных системах,		ния доступом в ком-	принципах управ-	лы знания о	управления доступом	
современные методы		пьютерных системах,	ления доступом в	принципах управ-	в компьютерных сис-	
защиты информации		современных мето-	компьютерных	ления доступом в	темах, современных	
при передаче ее по		дах защиты инфор-	системах, совре-	компьютерных	методах защиты ин-	
каналам связи, со-		мации при передаче	менных методах	системах, совре-	формации при пере-	
временные стандар-		ее по каналам связи,	защиты информа-	менных методах	даче ее по каналам	
ты информационной		современных стан-	ции при передаче	защиты информа-	связи, современных	
безопасности		дартах информаци-	ее по каналам свя-	ции при передаче	стандартах информа-	
31 (ОПК-3)		онной безопасности	зи, современных	ее по каналам свя-	ционной безопасно-	
			стандартах ин-	зи, современных	сти	
			формационной	стандартах ин-		
			безопасности	формационной		
				безопасности		
УМЕТЬ:	Отсутствие умений	Фрагментарные уме-	В целом успеш-	Успешное, но со-	Сформированное	Контрольные ра-
обосновать степень		ния обоснования сте-	ное, но не систе-	держащее отдель-	умение обоснования	боты
соответствия защи-		пени соответствия	матическое уме-	ные пробелы уме-	степени соответствия	
щаемых объектов		защищаемых объек-	ние обоснования	ние обоснования	защищаемых объек-	
информатизации и		тов информатизации	степени соответ-	степени соответ-	тов информатизации	
информатизацион-		и информатизацион-	ствия защищае-	ствия защищае-	и информатизацион-	
ных систем дейст-		ных систем дейст-	мых объектов ин-	мых объектов ин-	ных систем дейст-	
вующим стандартам		вующим стандартам	форматизации и	форматизации и	вующим стандартам	
в области информа-		в области информа-	информатизаци-	информатизаци-	в области информа-	
ционной безопасно-		ционной безопасно-	онных систем	онных систем	ционной безопасно-	
сти.		сти.	действующим	действующим	сти.	
У1(ОПК-3)			стандартам в об-	стандартам в об-		
			ласти информа-	ласти информа-		
			ционной безопас-	ционной безопас-		
			ности.	ности.		

ЗНАТЬ:	Не имеет базовых зна-	Допускает сущест-	Демонстрирует	Демонстрирует	Раскрывает полное	Отчеты, доклады
содержание процесса	ний о сущности про-	венные ошибки при	частичные знания	знания сущности	содержание процесса	на научных се-
целеполагания про-	цесса целеполагания,	раскрытии содержа-	содержания про-	процесса целепо-	целеполагания, всех	минарах
фессионального и	его особенностях и	ния процесса целепо-	цесса целеполага-	лагания, отдель-	его особенностей,	
личностного разви-	способах реализации.	лагания, его особен-	ния, некоторых	ных особенностей	аргументированно	
тия, его особенности		ностей и способов	особенностей	процесса и спосо-	обосновывает крите-	
и способы реализа-		реализации.	профессионально-	бов его реализа-	рии выбора способов	
ции при решении			го развития и са-	ции, характери-	профессиональной и	
профессиональных			мореализации	стик профессио-	личностной целереа-	
задач, исходя из эта-			личности,	нального развития	лизации при решении	
пов карьерного роста			указывает спосо-	личности, но не	профессиональных	
и требований рынка			бы реализации, но	выделяет крите-	задач.	
труда.			не может обосно-	рии выбора спо-		
31(УК-5(6))			вать возможность	собов целереали-		
			их использования	зации при реше-		
			в конкретных си-	нии профессио-		
			туациях.	нальных задач.		
УМЕТЬ:	Не умеет и не готов	Имея базовые пред-	При формулиров-	Формулирует це-	Готов и умеет фор-	Отчеты, доклады
формулировать цели	формулировать цели	ставления о тенден-	ке целей профес-	ли личностного и	мулировать цели	на научных се-
личностного и про-	личностного и профес-	циях развития про-	сионального и	профессионально-	личностного и про-	минарах
фессионального раз-	сионального развития	фессиональной дея-	личностного раз-	го развития, исхо-	фессионального раз-	
вития и условия их	и условия их достиже-	тельности и этапах	вития не учитыва-	дя из тенденций	вития и условия их	
достижения, исходя	ния, исходя из тенден-	профессионального	ет тенденции раз-	развития сферы	достижения, исходя	
из тенденций разви-	ций развития области	роста, не способен	вития сферы про-	профессиональ-	из тенденций разви-	
тия области профес-	профессиональной	сформулировать цели	фессиональной	ной деятельности	тия области профес-	
сиональной деятель-	деятельности, этапов	профессионального и	деятельности и	и индивидуально-	сиональной деятель-	
ности, этапов про-	профессионального	личностного разви-	индивидуально-	личностных осо-	ности, этапов про-	
фессионального рос-	роста, индивидуально-	тия.	личностные осо-	бенностей, но не	фессионального рос-	
та, индивидуально-	личностных особенно-		бенности.	полностью учи-	та, индивидуально-	
личностных особен-	стей.			тывает возмож-	личностных особен-	
ностей.				ные этапы про-	ностей.	
У1(УК-5(6))				фессиональной		
				социализации.		

Фонды оценочных средств, необходимые для оценки результатов обучения

Список вопросов для устного экзамена.

- 1. Метрические пространства, норма и метрика. Примеры.
- 2. Понятие сходимости в метрическом пространстве.
- 3. Понятие открытого и замкнутого множеств.
- 4. Компактность пространств и множеств: характеризация с помощью последовательностей.
- 5. Компактность пространств и множеств: характеризация с помощью открытых множеств.
- 6. Теорема Больцано-Вейерштрасса.
- 7. Теорема Гейне-Бореля.
- 8. Теорема Бэра.
- 9. Понятие динамической системы. Примеры.
- 10. Инварианты динамической системы. Примеры.
- 11. Дзета-функция динамической системы. Примеры вычисления дзета-функций для некоторых классов динамических систем.
- 12. Марковские рахбиения и символьное представления динамических систем.
- 13. Сдвиговые пространства(сдвиги) над конечным алфавитом. Полный сдвиг и другие примеры.
- 14. Характеризация сдвиговых пространств через множества запретов. Примеры.
- 15. Языки, порождаемые сдвигами. Критерии принадлежности слова языку. Неприводимые сдвиги.
- 16. Операция «расширения» сдвига и ее свойства.
- 17. Операция «расширения с зацеплением» сдвига и ее свойства.
- 18. Понятие скользящего блочного кода и его основные параметры. Примеры.
- 19. Понятие сопряженности сдвигов. Примеры.
- 20. Теорема о «гомоморфизме» для скользящего блочного кода.
- 21. Сверточные линейные коды. Примеры.
- 22. Сдвиги конечного типа. Примеры.
- 23. Сдвиги конечного типа с памятью. Примеры.
- 24. Критерий для сдвига конечного типа с памятью.
- 25. Теорема о свойствах сдвига сопряженного со сдвигом конечного типа.
- 26. Сдвиги, порождаемые конечными грфами, и их матричное описание. Примеры.
- 27. Теоретико-графовые представления сдвигов конечного типа. Теорема о представлении сдвига конечного типа с памятью графом.
- 28. Комбинирующий генератор, его основные параметры и свойства.
- 29. Фильтрующий генератор, его основные параметры и свойства.

- 30. Атаки на фильтрующий и комбинирующий генератор сизвестным открытым текстом. Методы реализации угроз.
- 31. Использование математических моделей символической динамики для описания комбинирующего генератора.
- 32. Использование математических моделей символической динамики для описания фильтрующего генератора.
- 33. Использование сопряженности для построения обратных отображений для скользящих блочных кодов, описывающих комбинирующие и фильтрующие генераторы.
- 34. Понятие энтропии сдвигового пространства и ее основные свойства.
- 35. Примеры вычисления энтропии для некоторых классов сдвигов..

Методические материалы для проведения процедур оценивания результатов обучения

Особенности организации процесса обучения

Для эффективного освоения курса рекомендуется перед каждым занятием прочитать конспект предыдущей лекции. После каждого занятия рекомендуется прочитать дополнительную литературу по теме лекции и привести в порядок свои конспекты.

Система контроля и оценивания

В каждом билете содержится 2 вопроса из приведенного в ФОС списка – 1-й на темы 1,2, а 2-й – на темы 3-5.

Структура и график контрольных мероприятий

Контрольные мероприятия в течение семестра отсутствуют.