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
имени М.В. Ломоносова

академик _____ И.А. Соколов

«___»_____ 2019 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Теория сложности вычислений»

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)

2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

1. НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ

Теория сложности вычислений

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 специальным дисциплинам вариативной части образовательной программы.

5. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций образовательной программы:

Формируемые компетенции	Планируемые результаты обучения
Способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности (ОПК-3)	З1 (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.
Способностью формулировать научные задачи в области обеспечения	З1(ОПК-1) ЗНАТЬ

информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность (ОПК-1);	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
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)	З1 (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 применять принципы информационной безопасности при разработке информационных систем	ЗНАТЬ: принципы информационной безопасности при разработке информационных систем **Код З1 (ПК-4)** УМЕТЬ: применять принципы информационной безопасности при разработке информационных систем **Код У1 (ПК-4)** ВЛАДЕТЬ: базовыми навыками выбора принципов информационной безопасности при разработке информационных систем **Код В1 (ПК-4)**

Оценочные средства для промежуточной аттестации приведены в Приложении.

6. ОБЪЕМ ДИСЦИПЛИНЫ

Объем дисциплины составляет 3 зачетныеt единицы, всего 108 часов.

24 часа составляет контактная работа с преподавателем – 22 часа занятий лекционного типа, 0 часов занятий семинарского типа (семинары, научно-практические занятия, лабораторные работы и т.п.), 0 часов индивидуальных консультаций, 0 часов мероприятий текущего контроля успеваемости, 0 часов групповых консультаций, 2 часа мероприятий промежуточной аттестации.

84 часов составляет самостоятельная работа аспиранта.

7. ВХОДНЫЕ ТРЕБОВАНИЯ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Учащиеся должны владеть знаниями по 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», 02.00.00 «Компьютерные и информационные науки».

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе обучения технические и программные средства не используются.

9. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

В курсе излагаются основные результаты и методы теории сложности вычислений. Основное внимание уделяется классам сложностей и отношениям между ними.

Наименование и	**Всего**	В том числе

краткое содержание разделов и тем дисциплины (модуля), **форма промежуточной аттестации по дисциплине (модулю)**	**(часы)**	**Контактная работа (работа во взаимодействии с преподавателем), часы** из них						**Самостоятельная работа обучающегося, часы** из них		
		Занятия лекционного типа	Занятия семинарского типа	Групповые консультации	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. Основные понятия теории сложности вычислений. Предмет теории сложности вычислений. Вычислительные задачи распознавания и поиска. Теоремы об ускорении и о линейном ускорении (формулировки). Важнейшие классы сложностей (DTIME(f), SPACE(f) NTIME(f), NSPACE(f), P, L, PSPACE, NP, NL, Σ_k^p, Π_k^p, PH). Сводимости по Куку и по Карпу. Полнота вычислительной задачи в классе сложностей относительно данной сводимости.	6	2					2		4	4
Тема 2. Иерархии класов сложностей. Функции, конструируемые по времени и по памяти. Теоремы об иерархии для классов	6	2					2		4	4

DTIME(f), SPACE(f), NTIME(f). Теорема о пропуске в иерархии (Gap Theorem).										
Тема 3. Вычисления с оракулами. Определение полиномиальной иерархии посредством машин Тьюринга с оракулами. Теорема Бейкера – Гилла – Соловея о релятивизированых классах P и NP. Теорема Беннетта – Гилла о классах, релятивизированных с помощью случайного множества. Соотношения между релятивизированными классами IP и PSPACE.	6	2					2		4	4
Тема 4. Вероятностные вычисления. Классы сложностей RP, BPP, ZPP, PP. Их место среди классов полиномиальной иерархии и PSPACE.	6	2					2		4	4
Тема 5. Неоднородные модели вычислений. Классы P/f и P/poly. Теорема Карпа – Липтона – Сипсера. Вычисления посредством булевых схем. Классы SIZE(f), NC^i и AC^i (однородные и неоднородные)ю	6	2					2		4	4
Тема 6. Теоремы Савича и Иммермана – Селепченьи. Теоремы Савича и Иммерма-	6	2					2		4	4

на – Селепченьи о задаче STCONN. Их важнейшие следствия для теории сложности вычислений.										
Тема 7. Задачи поиска. NP-отношения. Классы FNP и FP. Полнота FSAT в FNP. Самосводимость задач поиска. Самосводимость задачи FSAT. Примеры несамосводимых задач поиска из FNP. Пример языка из NP такого, что задача поиска, связанная с любым определяющим этот язык NP-отношением, несамосводима (в предположении EE≠NEE). Существование языков из NP, не принадлежащих P и не являющихся NP-полными (при подходящих предположениях).	8	2					2		6	6
Тема 8. Задачи подсчета числа решений. Класс #P. Parsimonious reduction. Примеры #P-полных задач относительной этой сводимости. Теорема Тоды (формулировка).	8	2					2		6	6
Тема 9. PCP-классы. Важнейшие PCP-классы. Задачи оптимизации и приближенные алгоритмы для них. PCP-теорема о классе NP и ее связь с приближенными алгоритмами для задачи MAX-3SAT.	8	2					2		6	6
Тема 10. Теория Ле-	8	2					2		6	6

вина сложности в среднем. Вероятностные задачи (distributional problems). Классы tpcP, tpcBPP, distP, distNP и sampNP. Сводимости по Куку и по Карпу для вероятностных задач. Пример полной задачи в классах distNP и sampNP.										
Тема 11. Теоретико-игровая характеризация класса PSPACE. Задачи TQBF и $TQBF_k$. Полнота TQBF в PSPACE и $TQBF_k$ в Σ_k^p.	8	2					2		6	6
12. Промежуточная аттестация – устный экзамен	32	2						30		
Итого	108	24						84		

10. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ УЧАЩИХСЯ

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

Литература для самостоятельной работы студентов в соответствии с тематическим планом .

Тема 1 «Основные понятия теории сложности вычислений»

- ✓ Arora S., Barak B. Computational complexity: A modern approach. – Cambridge University Press, 2007.
- ✓ Goldreich, O. Computational complexity: A conceptual perspective. – Cambridge University Press, 2008.

✓ Papadimitriou C. H. Computational complexity. – Addison-Wesley, 1994.
✓ Rudich S., Wigderson A. (eds.) Computational complexity. theory – IAS/Park City Mathematical Series, v. 10, American Mathematical Society, 2004.
✓ Крупский В. Н. Введение в сложность вычислений. М.: Факториал Пресс, 2006.
✓ Кузюрин Н. Н., Фомин С. А. Эффективные алгоритмы и сложность вычислений. Электронное издание, версия от 7 марта 2018 г. (http://discopal.ispras.ru/img_auth.php/f/f4/Book-advanced-algorithms.pdf).

Тема 2 «Иерархии класов сложностей»

✓ Arora S., Barak B. Computational complexity: A modern approach. – Cambridge University Press, 2007.
✓ Papadimitriou C. H. Computational complexity. – Addison-Wesley, 1994.
✓ Rudich S., Wigderson A. (eds.) Computational complexity. theory – IAS/Park City Mathematical Series, v. 10, American Mathematical Society, 2004.

Тема 3 «Вычисления с оракулами»

✓ Arora S., Barak B. Computational complexity: A modern approach. – Cambridge University Press, 2007.
✓ Goldreich, O. Computational complexity: A conceptual perspective. – Cambridge University Press, 2008.
✓ Baker T., Gill J., Solovay R. Relativizations of the P =? NP question. – SIAM J. Comput., 1975, 4(4), 431–442.
✓ Bennett C. H., Gill J. Relative to a random oracle A, $\mathbf{P}^A \neq \mathbf{NP}^A \neq \text{co-}\mathbf{NP}^A$ with probability 1. – SIAM J. Comput., 1981, 10(1), .96–113.
✓ Chang R., Chor B., Goldreich O., Hartmanis J., Håstad J., Ranjan J., Rohatgi P. The random oracle hypothesis is false, J. of Computer and System Sci., 1994, 49(1), 24–39.

Тема 4 «Вероятностные вычисления»

✓ Arora S., Barak B. Computational complexity: A modern approach. – Cambridge University Press, 2007.
✓ Goldreich, O. Computational complexity: A conceptual perspective. – Cambridge University Press, 2008.
✓ Кузюрин Н. Н., Фомин С. А. Эффективные алгоритмы и сложность вычислений. Электронное издание, версия от 7 марта 2018 г. (http://discopal.ispras.ru/img_auth.php/f/f4/Book-advanced-algorithms.pdf).

Тема 5 «Неоднородные модели вычислений»

✓ Arora S., Barak B. Computational complexity: A modern approach. – Cambridge University Press, 2007.
✓ Goldreich, O. Computational complexity: A conceptual perspective. – Cambridge University Press, 2008.
✓ Rudich S., Wigderson A. (eds.) Computational complexity. theory – IAS/Park City Mathematical Series, v. 10, American Mathematical Society, 2004.

Тема 6 «Теоремы Савича и Иммермана – Селепченьи»

✓ Arora S., Barak B. Computational complexity: A modern approach. – Cambridge University Press, 2007.

- ✓ Goldreich, O. Computational complexity: A conceptual perspective. – Cambridge University Press, 2008.
- ✓ Papadimitriou C. H. Computational complexity. – Addison-Wesley, 1994.
- ✓ Rudich S., Wigderson A. (eds.) Computational complexity. theory – IAS/Park City Mathematical Series, v. 10, American Mathematical Society, 2004.

Тема 7 «Задачи поиска»

- ✓ Goldreich, O. Computational complexity: A conceptual perspective. – Cambridge University Press, 2008.
- ✓ Papadimitriou C. H. Computational complexity. – Addison-Wesley, 1994.
- ✓ Bellare M., Goldwasser S. The complexity of decision versus search. – SIAM J. Comput., 1994, 23(1), 97–119.

Тема 8 «Задачи подсчета числа решений»

- ✓ Arora S., Barak B. Computational complexity: A modern approach. – Cambridge University Press, 2007.
- ✓ Goldreich, O. Computational complexity: A conceptual perspective. – Cambridge University Press, 2008.
- ✓ Papadimitriou C. H. Computational complexity. – Addison-Wesley, 1994.

Тема 9 «PCP-классы»

- ✓ Arora S., Barak B. Computational complexity: A modern approach. – Cambridge University Press, 2007.
- ✓ Goldreich, O. Computational complexity: A conceptual perspective. – Cambridge University Press, 2008.
- ✓ Rudich S., Wigderson A. (eds.) Computational complexity. theory – IAS/Park City Mathematical Series, v. 10, American Mathematical Society, 2004.
- ✓ Кузюрин Н. Н., Фомин С. А. Эффективные алгоритмы и сложность вычислений. Электронное издание, версия от 7 марта 2018 г. (http://discopal.ispras.ru/img_auth.php/f/f4/Book-advanced-algorithms.pdf).

Тема 10 «Теория Левина сложности в среднем»

- ✓ Arora S., Barak B. Computational complexity: A modern approach. – Cambridge University Press, 2007.
- ✓ Goldreich, O. Computational complexity: A conceptual perspective. – Cambridge University Press, 2008.
- ✓ Rudich S., Wigderson A. (eds.) Computational complexity. theory – IAS/Park City Mathematical Series, v. 10, American Mathematical Society, 2004.
- ✓ Goldreich O. Notes on Levin’s theory of average-case complexity. Electronic Colloquium on Computational Complexity (ECCC, https://eccc.weizmann.ac.il/), 1997, TR97-058.

Тема 11 «Теоретико-игровая характеризация класса PSPACE»

- ✓ Крупский В. Н. Введение в сложность вычислений. М.: Факториал Пресс, 2006.
- ✓ Arora S., Barak B. Computational complexity: A modern approach. – Cambridge University Press, 2007.
- ✓ Goldreich, O. Computational complexity: A conceptual perspective. – Cambridge University Press, 2008.

✓ Rudich S., Wigderson A. (eds.) Computational complexity. theory – IAS/Park City Mathematical Series, v. 10, American Mathematical Society, 2004.

11. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ

Основная литература

1. Arora S., Barak B. Computational complexity: A modern approach. – Cambridge University Press, 2007.
2. Goldreich, O. Computational complexity: A conceptual perspective. – Cambridge University Press, 2008.
3. Papadimitriou C. H. Computational complexity. – Addison-Wesley, 1994.
4. Rudich S., Wigderson A. (eds.) Computational complexity. theory – IAS/Park City Mathematical Series, v. 10, American Mathematical Society, 2004.
5. Крупский В. Н. Введение в сложность вычислений. М.: Факториал Пресс, 2006.
6. Кузюрин Н. Н., Фомин С. А. Эффективные алгоритмы и сложность вычислений. Электронное издание, версия от 7 марта 2018 г. (http://discopal.ispras.ru/img_auth.php/f/f4/Book-advanced-algorithms.pdf).

Дополнительная литература

1. Du D.-Z., Ko K.-I. Theory of computational complexity. – John Wiley & Sons, 2000.
2. Sipser M. Introduction to the theory of computation. – Thomson Course Technology, 2nd ed., 2006.

Ресурсы информационно-телекоммуникационной сети «Интернет»

1. http://discopal.ispras.ru/img_auth.php/f/f4/Book-advanced-algorithms.pdf
2. https://complexityzoo.uwaterloo.ca/Complexity_Zoo

Материально-техническая база

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

12. ЯЗЫК ПРЕПОДАВАНИЯ

Русский

13. РАЗРАБОТЧИК ПРОГРАММЫ, ПРЕПОДАВАТЕЛИ

к. ф.-м. н. Анохин Михаил Игоревич

Приложение

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

«Теория сложности вычислений »

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

Планируемые результаты обучения*	**Критерии и показатели оценивания результата обучения**					**Элемент (элементы) образовательной программы, формирующие результат обучения**	**Оценочные средства**
	1	2	3	4	5		
	Неудовлетворительно	**Неудовлетворительно**	**Удовлетворительно**	**Хорошо**	**Отлично**		
ЗНАТЬ: принципы управления доступом в компьютерных системах, современные методы защиты информации при передаче ее по каналам связи, современные стан-	Отсутствие знаний	Фрагментарные представления о принципах управления доступом в компьютерных системах, современных методах защиты информации при передаче ее по каналам связи, современных стандартах информационной безо-	В целом сформированные, но неполные знания о принципах управления доступом в компьютерных системах, современных методах защиты информации при передаче ее по каналам связи, со-	Сформированные, но содержащие отдельные пробелы знания о принципах управления доступом в компьютерных системах, современных методах защиты информации при передаче ее по каналам связи, современных стандартах	Сформированные систематические знания о принципах управления доступом в компьютерных системах, современных методах защиты информации при передаче ее по каналам связи, современных стандартах	Устный экзамен	ЗНАТЬ: принципы управления доступом в компьютерных системах, современные методы защиты информации при переда-

дарты информационной безопасности З1 (ОПК-3)		пасности	временных стандартах информационной безопасности	информационной безопасности	информационной безопасности		че ее по каналам связи, современные стандарты информационной безопасности З1 (ОПК-3)
УМЕТЬ: обосновать степень соответствия защищаемых объектов информатизации и информатизационных систем действующим стандартам в области информационной безопасности. У1(ОПК-3)	Отсутствие умений	Фрагментарные умения обоснования степени соответствия защищаемых объектов информатизации и информатизационных систем действующим стандартам в области информационной безопасности.	В целом успешное, но не систематическое умение обоснования степени соответствия защищаемых объектов информатизации и информатизационных систем действующим стандартам в области информационной безопасности.	Успешное, но содержащее отдельные пробелы умение обоснования степени соответствия защищаемых объектов информатизации и информатизационных систем действующим стандартам в области информационной безопасности.	Сформированное умение обоснования степени соответствия защищаемых объектов информатизации и информатизационных систем действующим стандартам в области информационной безопасности.	Контрольные работы	УМЕТЬ: обосновать степень соответствия защищаемых объектов информатизации и информатизационных систем действующим стандартам в области информационной безопасности. У1(ОПК-3)
ЗНАТЬ: научные задачи в области обеспечения информационной безопас-	Отсутствие знаний	Фрагментарные представления о научных задачах в области обеспечения информацион-	В целом сформированные, но неполные знания о научных задачах в облас-	Сформированные, но содержащие отдельные пробелы о научных задачах в области обеспече-	Сформированные систематические знания о научных задачах в области обеспе-	Устный экзамен	ЗНАТЬ: научные задачи в области обеспечения ин-

ности З1(ОПК-1)		ной безопасности	ти обеспечения информационной безопасности	ния информационной безопасности	чения информационной безопасности		формационной безопасности З1(ОПК-1)
УМЕТЬ: применять для задачи в области обеспечения ИБ решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность У1(ОПК-1)	Отсутствие умений	Фрагментарные умения применять для задачи в области обеспечения ИБ решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	В целом успешное, но не систематическое умение применять для задачи в области обеспечения ИБ решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	Успешное, но содержащее отдельные пробелы умение применять для задачи в области обеспечения ИБ решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	Сформированное умение применять для задачи в области обеспечения ИБ решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	Устный экзамен	УМЕТЬ: применять для задачи в области обеспечения ИБ решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность У1(ОПК-1)
ВЛАДЕТЬ: Навыками внедрения полученных результатов в практическую деятельность В1(ОПК-1)	Отсутствие навыков	Фрагментарное владение навыками внедрения полученных результатов в практическую деятельность	В целом успешное, но не полное владение навыками внедрения полученных результатов в практическую деятель-	Успешное, но содержащее отдельные пробелы владение навыками внедрения полученных результатов в практическую деятельность	Сформированное владение навыками внедрения полученных результатов в практическую деятельность	устный экзамен	ВЛАДЕТЬ: Навыками внедрения полученных результатов в практическую деятельность

			ность				В1(ОПК-1)
ЗНАТЬ: современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения З1 (ПК-1)	Отсутствие знаний	Фрагментарные представления о современных методах построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методах разработки и реализации алгоритмов их решения	В целом сформированные, но неполные знания о современных методах построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методах разработки и реализации алгоритмов их решения	Сформированные, но содержащие отдельные пробелы знания о современных методах построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методах разработки и реализации алгоритмов их решения	Сформированные систематические знания о современных методах построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методах разработки и реализации алгоритмов их решения	Устный экзамен	ЗНАТЬ: современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения З1 (ПК-1)
УМЕТЬ: применять современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработ-	Отсутствие умений	Фрагментарные умения применять современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реа-	В целом успешное, но не систематическое умение применять современные методы построения и анализа математических моделей, возникающих при решении естественнонона-	Успешное, но содержащее отдельные пробелы умение применять современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также совре-	Сформированное умение применять современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные	Контрольные работы	УМЕТЬ: применять современные методы построения и анализа математических моделей, возникающих при решении естественно-

ки и реализации алгоритмов их решения У1 (ПК-1)		лизации алгоритмов их решения	учных задач, а также современные методы разработки и реализации алгоритмов их решения	менные методы разработки и реализации алгоритмов их решения	методы разработки и реализации алгоритмов их решения		научных задач, а также современные методы разработки и реализации алгоритмов их решения У1 (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 В1 (ПК-1)	Отсутствие навыков	Фрагментарное владение 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	В целом успешное, но не полное владение 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	Успешное, но содержащее отдельные пробелы владение 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	Сформированное владение 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	Контрольные работы, реферат	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 В1 (ПК-1)
ЗНАТЬ: принципы ин-	Отсутствие знаний	Фрагментарные представления о	В целом сформированные, но	Сформированные, но содержащие от-	Сформированные систематические	Дисциплины вариативной части,	Устный экзамен

формационной безопасности при разработке информационных систем **Код З1 (ПК-4)**		принципах информационной безопасности при разработке информационных систем	неполные знания о принципах информационной безопасности при разработке информационных систем	дельные пробелы знания о принципах информационной безопасности при разработке информационных систем	знания о принципах информационной безопасности при разработке информационных систем	факультативные дисциплины	
УМЕТЬ: применять принципы информационной безопасности при разработке информационных систем **Код У1 (ПК-4)**	Отсутствие умений	Фрагментарные применять принципы информационной безопасности при разработке информационных систем	В целом успешное, но не систематическое умение применять принципы информационной безопасности при разработке информационных систем	Успешное, но содержащее отдельные пробелы умение применять принципы информационной безопасности при разработке информационных систем	Сформированное умение применять принципы информационной безопасности при разработке информационных систем	Исследовательская практика	Отчет
ВЛАДЕТЬ: базовыми навыками выбора принципов информационной безопасности при разработке информационных систем **Код В1 (ПК-4)**	Отсутствие навыков	Фрагментарное владение базовыми навыками выбора принципов информационной безопасности при разработке информационных систем	В целом успешное, но не полное владение базовыми навыками выбора принципов информационной безопасности при разработке информационных систем	Успешное, но содержащее отдельные пробелы владение базовыми навыками выбора принципов информационной безопасности при разработке информационных систем	Сформированное владение навыками базовыми навыками выбора принципов информационной безопасности при разработке информационных систем	Научные исследования	Отчет

Примечания:

*Категории «знать», «уметь», «владеть» применяются в следующих значениях:

«знать» – воспроизводить и объяснять учебный материал с требуемой степенью научной точности и полноты.

«уметь» – решать типичные задачи на основе воспроизведения стандартных алгоритмов решения;
«владеть» – решать усложненные задачи на основе приобретенных знаний, умений и навыков, с их применением в нетипичных ситуациях, формируется в процессе получения опыта деятельности.

Фонды оценочных средств, необходимые для оценки результатов обучения

Список вопросов для устного экзамена.

1. Введение. Предмет теории сложности вычислений. Вычислительные задачи распознавания и поиска. Теоремы об ускорении и о линейном ускорении (формулировки). Важнейшие классы сложностей (DTIME(f), SPACE(f), NTIME(f), NSPACE(f), P, L, PSPACE, NP, NL, Σ_k^P, Π_k^P, PH.
2. Функции, конструируемые по времени и по памяти. Теоремы об иерархии для классов DTIME(f), SPACE(f), NTIME(f). Теорема о пропуске в иерархии (Gap Theorem). Очевидные соотношения между классами сложностей.
3. Вычисления с оракулами. Определение полиномиальной иерархии посредством машин Тьюринга с оракулами. Теорема Бейкера – Гилла – Соловея о релятивизированных классах P и NP. Теорема Беннетта – Гилла о классах, релятивизированных с помощью случайного множества (формулировка). Соотношения между релятивизированными классами IP и PSPACE.
4. Вероятностные вычисления. Классы сложностей RP, BPP, ZPP, PP. Соотношения между ними. Место этих классов в полиномиальной иерархии.
5. Неоднородные модели вычислений. Классы P/f и P/poly. Теорема Карпа – Липтона – Сипсера (формулировка). Вычисления посредством булевых схем. Классы SIZE(f), NC^i и AC^i (однородные и неоднородные).
6. Теоремы Савича и Иммермана – Селепченьи о задаче STCONN. Их важнейшие следствия для теории сложности вычислений.
7. Задачи поиска. NP-отношения. Классы FNP и FP. Полнота задачи FSAT в FNP. Самосводимость задач поиска. Самосводимость задачи FSAT. Примеры несамосводимых задач поиска из FNP (при некоторых предположениях). Пример языка из NP такого, что задача поиска, связанная с любым определяющим этот язык NP-отношением, несамосводима (в предположении EE≠NEE). Существование языков из NP, не принадлежащих P и не являющихся NP-полными (при подходящих предположениях).
8. Задачи подсчета числа решений. Класс #P. Parsimonious reduction. Примеры #P-полных задач относительной этой сводимости. Теорема Тоды (формулировка).
9. PCP-классы. Задачи оптимизации и приближенные алгоритмы для них. PCP-теорема о классе NP (формулировка) и ее связь с приближенными алгоритмами для задачи MAX-3SAT.
10. Теория Левина сложности в среднем. Вероятностные задачи (distributional problems). Классы tpcP, tpcBPP, distP, distNP и sampNP. Сводимости по Куку и по Карпу для вероятностных задач. Пример полной задачи в классах distNP и sampNP.
11. Теоретико-игровая характеризация класса PSPACE. Задачи TQBF и $TQBF_k$. Полнота TQBF в PSPACE (формулировка). Полнота $TQBF_k$ в Σ_k^P.

Методические материалы для проведения процедур оценивания результатов обучения

Особенности организации процесса обучения

Для эффективного освоения курса рекомендуется перед каждым занятие привести в порядок конспекты лекций. После каждого занятия рекомендуется найти и прочитать дополнительную литературу по теме лекции и прочитать свои конспекты.