ТОкБиК

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО «СГУ имени Н.Г. Чернышевского»

Факультет компьютерных наук и информационных технологий

УТВЕРЖДАЮ
_____
«13» 04 2017 г.

Рабочая программа дисциплины
Сложность вычислений

Специальность
10.05.01 Компьютерная безопасность

Специализация
Математические методы защиты информации

Квалификация выпускника
Специалист по защите информации

Форма обучения
Очная

Саратов,
2017

1. Цели освоения дисциплины

Целью освоения дисциплины является проблемы математической логики, связанные с теорией вычислительных машин. Рассматриваются модели вычислительных устройств, их классификация, классификация языков, оценки сложности алгоритмов и вычислений. Второй целью являются приложения при создании стойких криптографических систем.

2. Место дисциплины в структуре ООП

Данная учебная дисциплина относится к вариативной части Блока 1 «Дисциплины (Модули)» ООП и направлена на формирование у обучающихся общепрофессиональных и профессиональных компетенций.

Для изучения дисциплины необходимы компетенции, сформированные в результате изучения дисциплин «Математическая логика и теория алгоритмов», «Дискретная математика», «Теория вероятностей и математическая статистика».

Компетенции, сформированные при изучении данной дисциплины, могут быть полезны при изучении дисциплин «Введение в криптоанализ».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины студент должен обладать следующими общепрофессиональными и профессиональными компетенциями:

- способностью к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах (ОПК-10).
- способностью осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов в сфере профессиональной деятельности (ПК-1).

В рамках указанных компетенций обучающийся должен

- Знать:

– сложностные классы P и NP;

– проблемы, разрешимые в полиномиальном пространстве;

- Уметь:

– применять методы оценки сложности вычислений для конкретно поставленных задач;

– разрабатывать быстрые вычислительные алгоритмы полиномиальной сложности для приложений;

- Владеть:

– навыком оценки сложности арифметических операций и основных алгоритмов;

– методами построения быстрых алгоритмов для реализации систем защиты информации.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы 108 часов.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля успеваемости (по неделям семестра) Формы промежуточной аттестации (по семестрам)
				Всего часов	Лекции	Лабораторные занятия	Самостоятельная работа	
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1	Введение. Неразрешимость в математической логике и в теории сложности вычислений	6	1	4	2	–	8	Коллоквиум на 4-й неделе
2	Машина Тьюринга, как вычислительная модель		2-3	8	4	–	8	
3	Классификация языков		4	6	2	–	8	
4	Сложностные классы *P* и *NP*		5-9	38	10	7	9	Контрольная работа на 9-й неделе
5	Емкостная сложность Классы *PS* и *NPS*..		10-12	18	6	2	9	Коллоквиум на 16-й неделе
6	Рандомизированные алгоритмы.		13	10	2	2	9	
7	Приложения в крипто графии		14-16	24	6	5	9	
	Промежуточная аттестация							Зачет
	ИТОГО			**108**	**32**	**16**	**60**	–

Введение. Неразрешимость в математической логике и в теории сложности вычислений.

Почему существуют неразрешимые проблемы во множестве языков над любым алфавитом.

Метод доказательства неразрешимости проблемы в математической логике путем сводимости.

Поиск решения всех проблем и теорема Геделя о неполноте.

“Неразрешимость” в теории сложности как невозможность решить проблему на компьютере.

Аксиомы функции сложности.

Машина Тьюринга, как вычислительная модель.

§ 1. Детерминированная машина Тьюринга.

§ 2. Языки, допускаемые одноленточной детерминированной машиной Тьюринга.

§ 3. Временная сложность, как число конфигураций машины Тьюринга.

§ 4. Полиномиальная временная сложность, или граница того, что можно решить с помощью компьютера.

§ 5. Многоленточная машина Тьюринга.

§ 6. Недетерминированная машина Тьюринга.

§ 7. Имитация машины Тьюринга на компьютере и компьютера на машине Тьюринга.

Классификация языков

§ 1. Неперечислимый язык.

§ 2. Коды машины Тьюринга.

§ 3. Язык диагонализации L_d.

§ 4. Рекурсивные языки.

§ 5. Универсальный язык L_u.

§ 6. Языки L_e и L_{ne}.

§ 7. Теорема Райса и свойства рекурсивно-перечислимых языков.

§ 8. Проблема соответствий Поста.

§ 9. Неразрешимость проблемы неоднозначности КС – грамматик.

Сложностные классы P и NP.

§ 1. Класс *P*. Проблемы, решаемые детерминированной машиной Тьюринга за полиномиальное время. Алгоритм Крускала. Сортировки.

§ 2. Класс *NP*. Проблемы, решаемые недетерминированной машиной Тьюринга за полиномиальное время.

§ 3. Полиномиальное сведение.

§ 4. *NP* – полные проблемы.

4.1. Проблема выполнимости булевой функции (ВЫП).

4.2. *NP* – полнота проблемы выполнимости КНФ (КНФ).

4.3. *NP* – полнота проблемы выполнимости 3-КНФ (3-КНФ).

4.4. Проблемы, к которым сводится проблема 3-КНФ:

Проблема независимого множества (НМ).

Проблема узельного покрытия (УП).

Проблема ориентированного гамильтонова цикла (ОГЦ).

Проблемы, к которым сводится проблема ОГЦ:

Проблема неориентированного гамильтонова цикла (НГЦ).

Проблема коммивояжера (ПК).

§ 5. Дополнения языков из классов *P* и *NP*: со-*P* и со-*NP*.

Емкостная сложность. Классы PS и NPS.

§ 1. Машины Тьюринга с полиномиальным пространством.

Классы *PS* и *NPS*.

§ 2. Связь *PS* и *NPS* с *P* и *NP*.

§ 3. *PS* - полнота. Проблема булевых формул с кванторами (КБФ).

Рандомизированные алгоритмы.

§ 1. Классы языков, основанных на рандомизации. Язык рандомизированной машины Тьюринга.

§ 2. Класс *RP*. Распознавание языков из *RP*.

§ 3. Класс *ZPP*. Соотношение между *RP* и *ZPP*

§ 4. Связь с классами *P* и *NP*.

Приложения в криптографии.

§ 1. Почему в криптографии используются проблемы, сложные “в среднем”, а не *NP*-полные.

§ 2. Сложность проверки простоты числа.

2.1. Рандомизированная полиномиальная проверка простоты.

2.2. Недетерминированные проверки простоты.

§ 3. Алгоритмы факторизации целых чисел.

§ 4. Криптосистемы, основанные на задаче о рюкзаке. Криптосистема Меркли-Хеллмана.

§ 5. Битовая стойкость. Сильные предикаты для дискретных алгоритмов.

План лабораторных работ

При выполнении лабораторной работы изучается теоретический материал, строится модель решаемой задачи и ее программная реализация, в частности с использованием языков программирования C++, C#, Java, Python. Приводится тестовый пример.

№ занятия	**Тема**	**Задания для лабораторного практикума**
1	Оценки сложности арифметических операций	[2], гл.1, §2
1	Сложность алгоритм Евклида, бинарного алгоритма Евклида Сложность расширенного алгоритма Евклида, бинарного расширенного алгоритма Евклида	[2]. гл.1, §2
2	Класс *P*. Проблемы, решаемые детерминированной машиной Тьюринга за полиномиальное время. Алгоритм Крускала. Сортировки.	[1], гл.4, стр.34-37.
2	*NP* – полные проблемы. Проблема выполнимости булевой функции (ВЫП). *NP* – полнота проблемы выполнимости КНФ (КНФ). *NP* – полнота проблемы выполнимости 3-КНФ (3-КНФ). Проблемы, к которым сводится проблема 3-КНФ: Проблема независимого множества (НМ). Проблема узельного покрытия (УП). Задача о сумме подмножеств (SUBSET-SUM) Проблемы, к которым сводится проблема ОГЦ: Проблема неориентированного гамильтонова цикла (НГЦ)	[1], гл.4, стр.38-57.
3	Емкостная сложность. Классы *PS* и *NPS*. Машины Тьюринга с полиномиальным пространством. Проблема булевых формул с кванторами (КБФ).	[1], гл. 5 стр.60-67

№ занятия	Тема	Задания для лабораторного практикума
4	Сложность проверки простоты числа. Рандомизированная полиномиальная проверка простоты. Недетерминированные проверки простоты.	[2], гл.3, §11
5	Алгоритмы факторизации целых чисел. Криптосистемы, основанные на задаче о рюкзаке. Криптосистема Меркли-Хеллмана.	[2], гл. 3, §13
6	Атаки на RSA, основанные на решетках	[2], гл.4, §14
7	Рандомизированные алгоритмы	[1], гл. 5 стр.65-71
8	Приближенные вычисления	[1], гл. 6 стр.72-80

5. Образовательные технологии, применяемые при освоении дисциплины

Предусматривается широкое использование в учебном процессе таких образовательных технологий как промежуточное тестирование, перекрестный опрос, использование методических материалов сайта кафедры теоретических основ компьютерной безопасности и криптографии, технологии анализа конкретных ситуаций. В рамках учебного курса предусмотрены встречи с представителями российских и зарубежных компаний, государственных и общественных организаций, мастер-классы экспертов и специалистов.

При обучении лиц с ограниченными возможностями здоровья и инвалидов используются подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуализации обучения, сопровождение тьюторами в образовательном пространстве; увеличивается время на самостоятельное освоение материала.

Основной формой организации учебного процесса является интегрированное обучение лиц с ограниченными возможностями здоровья и инвалидов, т.е. все студенты обучаются в смешенных группах, имеют возможность постоянно общаться со сверстниками, благодаря чему легче адаптируются в социуме.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

В рамках самостоятельной работы студенты

- изучают дополнительную литературу по предмету;
- занимаются научно-исследовательской работой.

Фонд оценочных средств дисциплины включает в себя задания для самостоятельной работы, задания для контрольной работы, контрольные вопросы, вопросы для проведения промежуточной аттестации (зачёт). Фонд оценочных средств дисциплины приведён в приложении 1.

7. Данные для учета успеваемости студентов в БАРС

Таблица 1 – Таблица максимальных баллов по видам учебной деятельности

1	2	3	4	5	6	7	8	9
Семестр	Лекции	Лабораторные занятия	Практические занятия	Самостоятельная работа	Автоматизированное тестирование	Другие виды учебной деятельности	Промежуточная аттестация	Итого
6	16	18	0	18	0	18	30	100

Программа оценивания учебной деятельности студента

6 семестр

Лекции

Оценивается посещаемость, активность – от 0 до 16 баллов.

Лабораторные занятия

Самостоятельность при выполнении работы, грамотность оформления, правильность выполнения и т.д. – от 0 до 18 баллов.

Практические занятия

Не предусмотрены.

Самостоятельная работа

Оценивается качество и количество выполненных работ, грамотность в оформлении, правильность выполнения – от 0 до 18 баллов.

Автоматизированное тестирование

Не предусмотрено

Другие виды учебной деятельности

Контрольная работа – от 0 до 18 баллов

Промежуточная аттестация

Промежуточная аттестация представляет собой теоретический зачёт, проводимый путем устного ответа на вопросы.

При проведении промежуточной аттестации

ответ на «отлично» оценивается от 24 до 30 баллов;

ответ на «хорошо» оценивается от 18 до 23 баллов;

ответ на «удовлетворительно» оценивается от 12 до 17 баллов;

ответ на «неудовлетворительно» оценивается от 0 до 11 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за шестой семестр по дисциплине «Сложность вычислений» составляет 100 баллов.

Таблица 2 – Таблица пересчета полученной студентом суммы баллов по дисциплине «Сложность вычислений» в оценку (зачет)

50 баллов и более	«зачтено»
Меньше 50 баллов	«не зачтено»

8. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1) Гамова, А. Н. Сложность вычислений [Текст] : учебное пособие для студентов и магистров факультета компьютерных наук и информационных технологий / А. Н. Гамова ; Сарат. гос. ун-т им. Н. Г. Чернышевского. - Саратов : Издательство Саратовского университета, 2015. - 79, [4] с. : ил., табл. - Библиогр.: с. 81 (6 назв.). - ISBN 978-5-292-04343-0.

б) дополнительная литература:

2) Черемушкин, А. В. Лекции по арифметическим алгоритмам в криптографии [Текст] : учеб. пособие / А. В. Черемушкин. - Москва : МЦНМО, 2002. - 103, [1] с. - Библиогр.: с. 100-103 (59 назв.). - ISBN 5-94057-060-7.

3) Гамова, А. Н. Математическая логика и теория алгоритмов [Текст] : учеб. пособие / А. Н. Гамова ; Сарат. гос. ун-т им. Н. Г. Чернышевского. - 2-е изд., доп. - Саратов : Изд-во Сарат. ун-та, 2000. - 78 с. - Библиогр.: с. 84 (6 назв.). - ISBN 5-292-03595-5.

г) программное обеспечение:

1) Лицензионное программное обеспечение: Visual C++ 4.2, Visual Studio 2010, Visual Studio 2012, Visual Studio 2013, Visual Studio 2015

2) Свободное программное обеспечение: Java Developers Kit, NetBeans IDE, Eclipse, CPython, Jython, IronPython.».

9. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий необходима лекционная аудитория с возможностью демонстрации электронных презентаций при уровне освещения, достаточном для работы с конспектом.

Для проведения лабораторных занятий необходим компьютерный класс с установленным программным обеспечением.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.01 Компьютерная безопасность и специализации «Математические методы защиты информации» (квалификация «Специалист по защите информации»).

Автор

Доцент кафедры теоретических основ компьютерной безопасности и криптографии, к.ф.-м.н., доцент _____ А.Н. Гамова

Программа разработана в 2012 г. (одобрена на заседании кафедры теоретических основ компьютерной безопасности и криптографии от «25» мая 2012 года, протокол № 18).

Программа актуализирована в 2017 г. (одобрена на заседании кафедры теоретических основ компьютерной безопасности и криптографии от «09» января 2017 года, протокол № 10).

Заведующий кафедрой теоретических основ компьютерной безопасности и криптографии, профессор, к.ф.-м.н. _____ В.Н. Салий

Декан факультета компьютерных наук и информационных технологий, к.ф.-м.н., доцент _____ А.Г. Федорова